A Multi-Stakeholder Dialogue on Age Assurance

Considerations Towards an Interoperable Age Assurance Framework

KEY TAKEAWAYS

13 June 2025

Key Takeaways
A Multi Stakeholder Dialogue on Age Assurance

Workshop on Interoperability

13 June 2025 | Brussels

The Multi-stakeholder Dialogue on age assurance, led by the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance, continues its commitment towards identifying emerging best practices in age assurance that can build a common and interoperable framework through dialogues and focused workshops.

This Workshop on Interoperability provided an overview of the current landscape and future directions for age assurance. It also discussed a draft interoperability framework developed in the Multi-stakeholder Dialogue and sought feedback from stakeholders who participated in the workshop. The conversation revolved around two main parts: (i) the proposed age assurance framework and (ii) specific considerations for viable age assurance beyond 18+ verification.

Below are the key takeaways.

Key Takeaways

As digital platforms continue to play a central role in the lives of children and young people, the need for effective, privacy-respecting age assurance continues to be a central point of discussion. Age assurance is not just a means to prevent children from accessing restricted content; it is a risk mitigation measure, often also necessitated by legal obligations. Yet the landscape for age assurance is becoming more and more complex, marked by new legal obligations, codes or guidance at increasing intervals, inconsistent technical implementations, a lack of interoperability, and limited user control.

This, coupled with age limits varying across jurisdictions, creates challenges for services operating globally and burdens user experiences.

There is a growing consensus to address these challenges. A more unified, standards-based framework for age assurance is needed. Such a framework should be **interoperable across services and jurisdictions**, offer **flexibility for developers** and **minimise personal data collection** while providing trustworthy age assurance and a more uniform user experience.

CIPL and WeProtect Multi-stakeholder Dialogue on Age Assurance has explored what such a broader interoperability framework for age assurance could look like, connecting different credential holders with an application or online service.

Main Elements of the Draft Interoperable Framework

- Digital credentials can be based on a number of sources, including governments and private issuers as well as providers of age estimation techniques offering choices and flexibility in age assurance as technology continues to evolve.
- A framework should be **technologically neutral**, aiming for broad applicability across industry applications.
- Age assurance must be **proportionate and risk-based**, meaning the level of age assurance (e.g., age verification vs. estimation) should be commensurate with the associated risk of the service or content.
- **Transparency**: Users must receive clear explanations about why age assurance is required and how it works.
- **User Autonomy**: Users should be empowered to choose whether to share assurance information with a particular relying party and which suitable credential they wish to share for verification, enhancing user agency as well as their overall experience.
- Users should have sufficient **redress mechanisms** available to challenge age assurance decisions, and control over the sharing of their age information.
- **Privacy by design** constitutes a fundamental principle of any interoperable solution. Privacy Enhancing Technology (PETs) such as Zero Knowledge Proof (ZKP) technology offer additional privacy protections, minimising data sharing and ensuring that credential holders cannot track user activity.
- **Security:** The framework should have the appropriate mechanisms in place to prevent misuse and protect from bad actors who might try to exploit the system.
- **Defines Roles and Liability Undertakings**: All the roles and the liability of each party involved in the operation of the framework should be clearly defined:
  - Age assurance providers should be responsible for the validity of signals;
  - API providers are responsible for the technical integrity of the API and supporting interoperability as feasible, and
  - App developers/website providers for implementing appropriate measures based on their risk assessments.

Additional Considerations for an Interoperable Framework

The workshop provided an opportunity for stakeholders to engage in a meaningful discussion, gathering their insights on additional key elements to be considered for an interoperable framework.

Below some of the main takeaways:

Ensuring fair competition, cost allocation, and clarity on liability

- Where relevant, a framework should address the commercial relationships between age assurance providers and relying parties (e.g., apps or websites) as the current practice involves direct contracts between a website or service and a verification provider.
- The framework should be inclusive and open to a multitude of solutions or signals to ensure broad utility and healthy competition, with standards that do not inadvertently exclude smaller players from participating.
- Cost allocation for the continued maintenance and functionality of a framework and the underlying technology will have to be addressed, as well as liability in case of potential negligence or errors.
- The workshop recognised a general need to move towards clear standards and accreditation of trusted signals to establish trust in the available solutions.
- An interoperable framework will be most effective if it is flexible enough to empower online platforms to comply with diverse regulatory requirements across jurisdictions.

Cross-Sector Collaboration

- The success of an interoperability framework for sharing age signals depends on cross-sector cooperation to ensure systems are compatible, reduce friction for users, and create overall a cohesive and well-integrated experience for all stakeholders.
- A key challenge will be to identify what would constitute a trusted signal and what the accreditation process would involve. This requires active engagement of stakeholders, including:
    - those who currently provide age signals,

- those with the potential to do so (e.g. financial institutions, telecommunication providers),
- regulators who should acknowledge and define which signals can be accepted as part of an interoperable framework, and
- accreditation or verification of actors to ensure that the accepted signals meet the agreed standards.

The role of regulators

- Regulators should foster a common understanding and taxonomy of age assurance methods. This will lead to a uniform framework that can bridge existing regulatory gaps and enable broad applicability.
- Regulators should also be open to innovative approaches, such as pilot projects and sandboxes to test a framework's effectiveness in real-world scenarios.

The role of PETs

- Stakeholders recognised the important role of PETs to limit unnecessary data sharing. However, where an age signal is incorrect or a minor gains access to non-age-appropriate content, PETs prevent tracing the origin of the age information, which hinders online providers' ability to mitigate and ensure accuracy.
- To address this issue, a framework should consider complaint or reporting mechanisms to allow issue flagging to the signal provider in the case of conflicting age signals. For example, where a user's behaviour on a given platform indicates that they may be below (or above) the age provided through the age signal,[3] or where an age signal turns out to be inaccurate or compromised, these mechanisms would be crucial for the continuous improvement and accuracy of age assurance solutions. This should go hand in hand with overall detailed and robust appeal procedures on individual services or apps.

Valuable Age Signals for Effective Age Assurance

Children under 18 years old engage with the digital world in diverse and complex ways, which necessitates approaches that are tailored to their developmental stages. The 13 to 18 age group presents a unique challenge: it is a broad and ambiguous range where months, not just years, can make a significant difference in cognitive maturity, and online behaviour, and move an individual from one legal threshold to the next.

Children below 13 years old often also participate in the online world; appropriate engagement will generally depend on parental supervision of this age group.

As there are a few jurisdictions in which digital IDs are issued to those below 18 years old,[4] there is a need to explore more signals that can support age assurance in the 13 to 18 age range (and potentially below) to ensure that children can navigate the online world safely. These signals may indicate a user's likely age with some precision or come in the form of age bands, as appropriate. The level of access or safeguards may in some cases require granularity. Age assurance should not be an exclusionary tool but instead should be seen as a tool for risk mitigation that aims to support age-appropriate content.

A number of sources could provide signals to be deployed in the 13+ age assurance context:

- **Mobile phone service providers** and **financial institutions** can play a constructive role by contributing to trusted age signals based on their existing customer data and relationships. Mobile phone contracts and bank accounts also often establish a direct, reliable link between a parent and child,[5] potentially covering a large proportion of young users.

- **Government-held information**, such as social security, educational or health records. Of course, public bodies are often reluctant to share sensitive data, and existing GDPR purpose limitation rules restrict using data collected for one purpose (e.g., education) to be used for another (e.g., age assurance) unless the new purpose is compatible with the original.

Age Assurance Considerations Beyond Age Signals

Ongoing Concerns in Age Assurance

The workshop also focused on additional consideration for sustainable solutions to age assurance.

Risk-based approach

- A risk-based approach is fundamental to effective age assurance: it is critical for tailoring protective measures to the potential risks of online services. Risk-based approach will remain central to policy discussions as technology evolves and risks shift over time.

- For example, the rapid development of AI tools creates new challenges, such as complex issues around identity verification (e.g., determining whether the user is human), that need to be carefully considered when crafting age assurance solutions.

Parental engagement

- Parents come from different cultural and socioeconomic backgrounds and may not all have the same level of digital maturity or attitude to their children's online engagement. Many parental control tools can be complex to understand, and because they differ across platforms, using them effectively may require significant time and effort. This raises and will continue to raise questions about how to provide meaningful assistance to parents when navigating this environment.

- There should be a careful balance between the necessary levels of parental engagement and provider responsibility when it comes to developing and implementing accessible age assurance measures and parental control tools. Parents and guardians have the discretion to decide what their children should access online.

Next Steps

CIPL and WeProtect Multi-stakeholder Dialogue is an ongoing project. Next steps include exploring further alignments on standards and protocols in the context of the interoperability framework.

For more information please contact Zeta Rizikianou (grizikianou@hunton.com) and Alison McNulty (alison@weprotectga.org).

End Notes

[1] The UK Age Appropriate Design Code (AADC) requires online services "likely to be accessed by children" to "establish the age of child users with a level of certainty that is appropriate for the risks your data processing creates." Please see: Information Commissioner's Office (ICO), "Age Assurance – Estimating or Verifying the Age of Service Users," in Children's Code: Best Interests Framework, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/age-assurance/

[2] Below are some recent examples of new legal obligations and initiatives to develop new codes:

- In July 2025, the European Commission published the guidelines on the protection of minors under Article 28(4) of the Digital Services Act, following a consultation that gathered input from all interested stakeholders. Please see: European Commission. Commission Publishes Guidelines on the Protection of Minors. July 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
- Additionally, on the EU level eIDAS 2 Regulation is progressing. The regulation mandates EU Member States to provide EU Digital Identity Wallets.
- The OAIC is developing a Children's Online Privacy Code, expected to be finalised in 2026, and launched a consultation to gather feedback from industry, children, parents, civil society, academia, and other stakeholders. Please see: Office of the Australian Information Commissioner (OAIC), Children's Online Privacy Code: Consultation for Industry, Civil Society, Academia and Other Interested Stakeholders, https://www.oaic.gov.au/engage-with-us/consultations/childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia-and-other-interested-stakeholders
- The Office of the Privacy Commissioner of Canada (OPC) launched a consultation to inform the creation of a federal Children's Privacy Code clarifying obligations under PIPEDA, and is seeking input from industry, parents and guardians, child-rights groups, educators, and youth to ensure its provisions reflect practical challenges and protect children's interests. Please see: Office of the Privacy Commissioner of Canada, *Exploratory Consultation on a Children's Privacy Code*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-children-code/expl_children-code/
- From 25 July 2025, platforms must use effective age assurance mechanisms to block children from harmful content, including pornography, self-harm, suicide, eating disorders, bullying, hate speech, dangerous stunts, or ingesting harmful substances. They must also offer clear reporting tools for parents and children. Please see: *Online Safety Act*, collection page, GOV.UK (Department for Science, Innovation and Technology), published 24 July 2025, https://www.gov.uk/government/collections/online-safety-act
- On October 2024, France's regulator ARCOM published a binding age verification standard for pornographic sites, mandating robust, privacy-preserving measures such as double anonymity, with full compliance required by 11 April 2025. Please see: Osborne Clarke. (2025, January 9). *French regulator Arcom's standard for online age verification rolls out in 2025*. https://www.osborneclarke.com/insights/french-regulator-arcoms-standard-online-age-verification-rolls-out-2025
- Spain released technical specifications for an age verification system using W3C Verifiable Credentials to ensure GDPR-compliant, privacy-preserving proof of age for accessing adult content. Please see: Ministerio para la Transformación Digital y de la Función Pública. *Especificaciones técnicas*. https://digital.gob.es/especificaciones_tecnicas.html
- Greece launched the Kids Wallet app as part of its National Strategy for the Protection of Minors, enabling parents to manage children's digital access through parental controls linked to official digital identity systems. Please see: Ministry of Digital Governance. (2025). *Protecting minors from internet addiction: National strategy*. Hellenic Republic. https://mindigital.gr/wp-content/uploads/2025/03/%CE%9DStrategy_ProtectM_long_ENG.pdf

[3] For example, providing a "contra indicator" or "red flag" based on community moderators or peer reporting.

[4] In Denmark, from the age of 13, individuals in Denmark can obtain MitID, the national digital ID, which allows access to certain self-service platforms such as online banking or tax services—though some services remain restricted until the age of 15.Please see: MitID, "13 to 14 Years Old," *MitID Help Universe*, https://www.mitid.dk/en-gb/help/help-universe/13-to-14-years-old/.
In India, there is no age limit for obtaining the Adhaar Card (a unique identification document issued by the Government of India); individuals of any age, even newborns can enrol for one. This system is beneficial as it helps in availing various government services and schemes from an early stage. Please see: "Aadhaar Card Age Limit," *Bajaj Finserv*, https://www.bajajfinserv.in/aadhaar-card-age-limit

[5] This is because children cannot open an account or enter into a contract without parental consent. The age limit varies across jurisdictions.

Who We Are

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

WeProtect Global Alliance brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.