Global Age Assurance Standards Summit 2025

Summit Communiqué Final

Global Age Assurance Standards Summit – Summit Communiqué

Date: May 22, 2025
Location: Amsterdam, NL

Communique

Global Age Assurance Standards Summit

The Global Age Assurance Standards Summit between April, 8 2025 and April, 10 2025, has brought together interested parties including governments, regulators, international organisations, civil society, academia, industry leaders, age assurance service providers, standards developers and technical experts to prepare this communique to reflect the position, state of the art and development of age assurance standards as at May, 22 2025.

Building on the Headline of the inaugurate Summit Communique in April 2024 that 'Age Assurance can be done', the 2025 Summit Communique goes further and shows the state of play as having moved on significantly in the space of one year:

Headline

Age Assurance can be done.

Age Assurance can be deployed, with the right process that recognises the specific context and use case, in a manner that is privacy preserving, data minimising, secure, effective and efficient.

Age assurance can be a valuable tool amongst a range of measures deployed to protect children in the digital environment.

Global Age Assurance Standards can help local Regulation to work well.

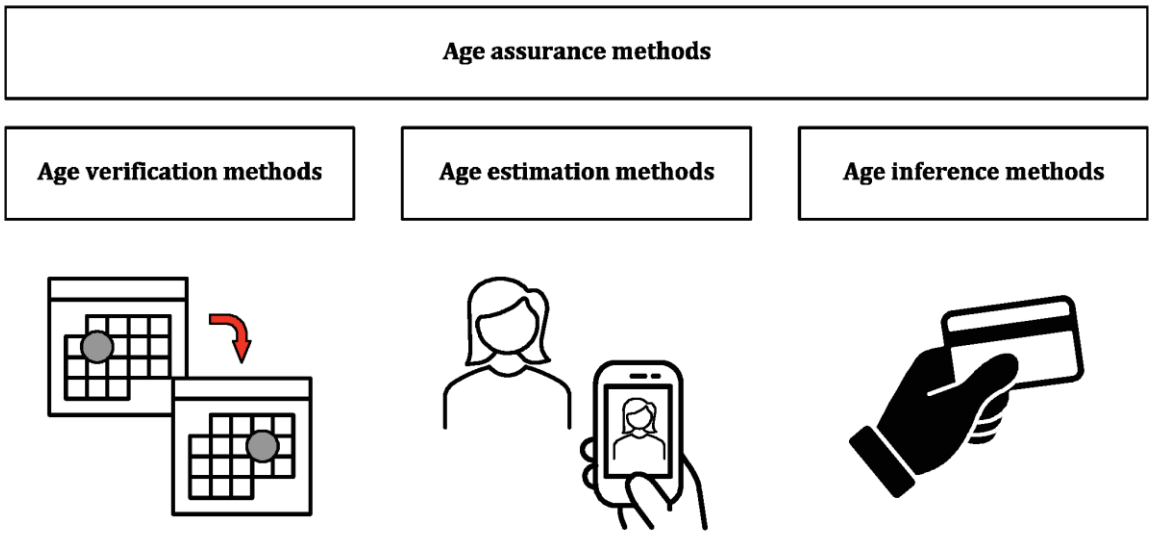
This would be assisted by securing International Standards, which are implemented and respected by providers of services that are required to make age related eligibility decisions.

Laws and regulations can create the legal framework with robust enforcement procedures in place to secure the protection of children from harm.

If deployed proportionately and effectively, Age Assurance represents an opportunity to enhance the fundamental rights of children in a digital age, in addition to protecting anonymity and the freedoms of adults to enjoy online goods, content and services.

Definition

Age assurance is a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make age-related eligibility decisions with varying degrees of certainty [ISO/IEC DIS 27566-1]



Calculating the difference between a verified year or date of birth of an individual and a subsequent date	Analysis of biological or behavioural features of humans that vary with age	Verified information which indirectly implies that an individual is over or under a certain age or within an age range

Preamble

Whereas the UN Committee of the Rights of the Child outlined the range of rights at play for children in the digital environment in General comment No. 25 (2021) on children's rights in relation to the digital environment of March, 2 2021 (CRC/C/GC/25).

Recalling General Comment No. 20 on the implementation of the rights of the child during adolescence (CRC/C/GC/20), in which the United Nations recognized the importance of protecting children from all forms of violence, abuse and exploitation in the digital environment.

Noting the work of the United Nations Commission on International Trade Law, Working Group IV: Electronic Commerce addressing identity and trust services [UN/A/CN.9/WG.IV].

Acknowledging the recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

The CEN CENELEC specification on age appropriate design makes reference to the need for all age assurance systems to protect the privacy of users in accordance with applicable laws, including human rights laws. [CEN-CENELEC CWA 18016 Age Appropriate Digital Services Framework] [1]

The EU Artificial Intelligence Act follows a product safety approach, but with the new added element of a fundamental rights impact assessment. The first EU Commission standardisation request includes obligations related to fundamental rights and data protection. Standardisation bodies such as ETSI [STF 681(TCHF) Special Task Force on Age Verification] are already moving

[1] Based on the CWA on April 1st, 2025 CEN/CENELEC have started the process of developing a European Standard (EN) by adoption of a Preliminary Work Item in the committee's work programme, CEN/CLC JTC 13 – Cybersecurity and data protection.

towards harmonised global standards on AI which are underpinned by the EU AI Act and are likely to include a requirement to consider fundamental rights impacts.

Noting that where age assurance tools are deployed that in many cases they will also be used by adults in order to determine that they are not a child (for example when accessing pornography sites, gambling sites, or when purchasing age restricted goods). The 9 core international human rights instruments apply in this context to all adult and child users.

Noting the UN Guiding Principles (UNGPs) on Business and Human Rights set out the responsibility of companies to respect human rights and children's rights in the digital environment.

Recalling the guide on Article 8 of the European Convention on Human Rights right to respect for private and family life, home and correspondence from the European Court of Human Rights, updated on 31 August 2024.

Recalling the EU Digital Services Act (DSA) Article 28 on Online protection of minors from October, 19 2022.

The Convention on the Rights of the Child and its Optional Protocols, as well as other relevant international human rights instruments, provide the legal framework for the promotion and protection of the rights of the child in the online context.

Acknowledging the benefits and opportunities that the digital environment offers for children's education, participation, creativity, expression and social inclusion, as well as the challenges and risks that it poses for their safety, privacy, well-being and development.

Noting with concern the increasing availability and accessibility of online services that may expose children to illegal or harmful content, such as pornography, violence, gambling, or products such as alcohol and tobacco, or that may collect, process or share their personal data without their consent, knowledge or understanding.

Noting with concern the existence of online platforms where children are exposed to the malice of adults.

Recognising the need for a global, coordinated and multi-stakeholder approach to ensure that online services are designed and delivered in a way that respects and protects the rights and best interests of the data subject, taking into account their evolving capacities and the diversity of their situations and needs.

Noting further the technical difficulties created by synthetic data and the need for any such standards to be responsive to developments in technology.

Welcoming the efforts of various actors, such as governments, regulators, international organisations, civil society, academia, industry and technical experts, to develop and implement age assurance regulations, mechanisms and standards for online services, which include specifications for self declaration, age estimation, age verification and age appropriate design.

Acknowledging the efforts of the International Standards Organisation through ISO/IEC JTC 1/SC 27/WG 5 to develop international standards for age assurance, most specifically:

- ISO/IEC DIS 27566 - 1 - Age Assurance Systems - Part 1: Framework
- ISO/IEC PWI 27566 - 2 - Age Assurance Systems – Part 2: Technical approaches and guidance for implementation
- ISO/IEC WD 27566 - 3 - Age Assurance Systems - Part 3: Comparison or Analysis

Acknowledging the efforts of the Institute of Electrical and Electronics Engineers to develop a global standard IEEE 2089.1-2024 Standard for Online Age Verification.

Call to Action

Bearing in mind the principles of necessity, proportionality, transparency, accountability and non-discrimination in the application of age assurance measures, as well as the respect for the views and preferences of the child and the role of parents, guardians and caregivers.

The Global Age Assurance Standards Summit identified that relevant parties and stakeholders should:

1. Encourage the voluntary adoption and certification of age verification solutions aligned with internationally recognized standards (e.g., ISO 27566, IEEE 2089.1) to promote interoperability, trust, and accountability.

2. Embed privacy-by-design principles in all age assurance systems, leveraging privacy-enhancing technologies such as zero-knowledge proofs, and decentralized identity models to protect user data while ensuring compliance.

3. Develop and support mutual recognition frameworks for digital identities (including an age attribute) to reduce regulatory fragmentation, streamline compliance, and improve access to safe digital experiences across jurisdictions.

4. Ensure robust, transparent, and independently certified age assurance technologies are affordable and accessible worldwide, including the Global South by supporting and integrating mobile-based verification, national ID system integration, and alternative assurance models. This may be particularly important in countries where a mobile and/or shared device will be the principle or only means of connecting to the internet.

5. Where governments and regulatory authorities decide to require online platforms and digital service providers to implement age assurance measures, these should incentivize compliance through clear regulations, standardization, and recognition of best-practice providers.

6. Support research into privacy-preserving, data minimising, user friendly age assurance systems, ensuring compliance with international human rights, global ethical and accountability frameworks to prevent bias and discrimination while enhancing privacy, safety, and security.

7. Decide to remain seized of the matter.

International Age Assurance Standards

The international age assurance standards are a set of principles and guidelines for the development and implementation of age assurance mechanisms and standards for age related eligibility decisions. They are based on the existing and emerging good practice and initiatives in this field, as well as on the relevant international human rights instruments, especially the United Nations Convention on the Rights of the Child and its Optional Protocols. They aim to provide a common reference framework and a shared vision for all actors involved in the design and delivery of online services, and to foster a global, coordinated and multi-stakeholder approach to ensure that online services are respectful and protective of the rights and best interests of the child.

The international age assurance standards are voluntary and flexible, and they do not intend to prescribe or impose any specific technical or legal solutions. They recognize that different

contexts and situations may require different levels of approaches and methods and that age assurance is not a one-size-fits-all, silver bullet solution. They also acknowledge that age assurance is not a panacea or a substitute for other measures and actions to protect children online, such as education, awareness-raising, parental guidance and support and effective law enforcement.

Guiding Principles

The Global Age Assurance Standards Summit has identified these six main principles and eighteen guidelines, as follows:

Principle 1: Human rights and best interests of the individual

Guideline 1.1: Age assurance systems should aim to protect and promote the rights and best interests of the individual in the online environment, in accordance with relevant international human rights instruments.

Guideline 1.2: When considering age assurance implementation, platforms and service providers should balance the protection and the empowerment of the individual and should not unduly restrict or limit their access to online services that are beneficial or appropriate for their age, development and well-being.

Guideline 1.3: When considering age assurance implementation, platforms and service providers should take into account the evolving capacities and the diversity of situations and needs of children of different ages, backgrounds and circumstances and should respect their views and preferences.

Principle 2: Risk-Based and Proportionate Implementation

Guideline 2.1**:** Platforms and service providers must recognise that the implementation of age assurance comes with the obligation to do a risk assessment and human rights impact assessment first, asking the question of 'What level of risk does my service entail, do I need age

assurance as a result, if so what level of age assurance do I need and what impact does this have on human rights?'

Guideline 2.2: Age assurance mechanisms should be adaptable to different regulatory environments.

Guideline 2.3: Regulatory authorities should provide clear regulatory guidance on proportionate age assurance requirements for different content, products, and services.

Principle 3: Privacy-Preserving by Design

Guideline 3.1: Age assurance systems must incorporate privacy-preserving technologies such as Zero-Knowledge Proof (ZKP) or decentralized identity models, and avoid excessive data processing.

Guideline 3.2: Governments and industry stakeholders should adhere to the highest privacy regulations (e.g., GDPR, COPPA, UK ADC).

Guideline 3.3: Data minimization should be a core requirement, ensuring that only the necessary information is used for the age assurance process.

Principle 4: Standards-Based Interoperability

Guideline 4.1: Regulatory authorities should adhere to internationally recognized standards such as ISO 27566-1 and IEEE 2089.1 to facilitate cross-border interoperability.

Guideline 4.2: Mutual recognition of digital identities – including an age attribute – should be promoted to streamline compliance and enhance user access to age-appropriate services.

Guideline 4.3: Industry and regulatory bodies should collaborate with relevant stakeholders – including self-regulatory bodies and civil society organisations on certification programs that ensure age verification solutions meet global interoperability requirements.

Principle 5: Digital Inclusion and Accessibility

Guideline 5.1: There must be age assurance solutions accessible to all users, ensuring affordability and ease of use.

Guideline 5.2: Alternative verification methods, such as mobile-based identity and/or age verification, national ID integration, and community-driven models, must be developed to ensure availability also where digital infrastructure might be weak.

Guideline 5.3: Capacity-building initiatives and knowledge-sharing programs should support the implementation of effective age assurance especially in emerging digital economies.

Principle 6: Transparency, Accountability, and Innovation

Guideline 6.1: If online platforms and service providers implement age assurance measures, these must be independently certified, ensuring transparency and accountability in regard of handling the user data.

Guideline 6.2: Regulatory frameworks should encourage continuous innovation in age assurance technologies while maintaining ethical safeguards against bias and discrimination.

Guideline 6.3: Governments should incentivize compliance, for instance through regulatory guidance, recognition of best-practice providers, etc..

This communiqué is co-authored and handed over by the project "Child Protection and Children´s Rights in the Digital World".

Project Managment
- Jutta Croll, ++49-163-5493-773, jcroll@digitale-chancen.de
- Torsten Krause, ++49-176-8493-4885, tkrause@digitale-chancen.de

More information
www.childrens-rights.digital

childrens-rights.digital