Protection of Minors – CCIA Europe's Recommendations on Age Assurance

Helping Europe achieve safe and secure age-assurance solutions

February 2025

The Computer & Communications Industry Association (CCIA Europe) and its Members are committed to ensuring minors are protected online and are granted a high level of safety, security, and privacy in their online experiences. Achieving this requires continued efforts and ongoing collaboration across the internet ecosystem.

One key aspect under discussion at EU level is age assurance: its necessity, application, and how to balance requirements of safety, privacy, and reliability. While age assurance is important, it should coexist with other solutions like parental controls. As the EU seeks to strengthen minor protection, taking into account the existing framework established by the Digital Services Act (DSA), Audiovisual Media Services Directive (AVMSD), and other non-legislative initiatives, CCIA Europe shares these age-assurance recommendations.

I. Consider the risk profiles of different online services

No online service is like another, and not every service holds the same risk when minors use or access content through it. A risk-based approach to any age-assurance requirements is therefore essential to ensure that services presenting the greatest risks to minors also take on the highest level of responsibility.

II. Ensure uniform implementation of the European electronic identity framework

As the EU prepares for the full implementation of Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS Regulation), the European Commission must provide clear guidelines for Member States on how to implement electronic identification means. This will prevent fragmentation and ensure interoperability across the European Union.

III. Provide transitional solutions that balance safety and privacy

While the eIDAS framework has the potential to complement existing age-assurance measures, its full implementation – and potential uptake – remain a work in progress. During this transition, online services must be able to rely on solutions that fulfil the same requirements for accuracy, security, and privacy protection for all users.

Introduction

The Computer & Communications Industry Association (CCIA Europe) and its Members are deeply committed to the protection of minors online, and firmly believe that minors should be granted a high level of safety, security, and privacy in their online experiences. In order to make sure that minors have the most positive experience, continued efforts and ongoing collaboration are necessary by all players across the internet ecosystem.

One aspect of minor protection that is currently heavily discussed at the European level is age assurance[1] – in particular to what extent it is needed as an instrument to increase minors' safety and security online. The debate also focusses on who would need to apply such assurance methods, as well as necessary guarantees in terms of privacy, security, reliability, and overall online safety.

It has to be stressed that age assurance is only one piece of the puzzle, and should co-exist with other solutions such as parental controls. Although no aligned age-assurance framework exists yet, we must find ways to protect minors online and ensure their experiences are suitable and appropriate for their age and maturity.

As the European Union is working on measures to streamline the protection of minors on the internet – and taking into account the legal framework established by the Digital Services Act (DSA),[2] the Audiovisual Media Services Directive (AVMSD),[3] and other non-legislative EU initiatives – CCIA Europe respectfully offers the following recommendations on age assurance.

I. Consider the risk profiles of different online services
II. Ensure uniform implementation of the European electronic identity framework
III. Provide transitional solutions that balance safety and privacy

I. Consider the risk profiles of different online services

No online service is like another, and not every service holds the same risk when minors use or access content through it. A risk-based approach to any age-assurance requirements is therefore essential to ensure that services presenting the greatest risks to minors also take on the highest level of responsibility.

CCIA Europe considers that while age assurance could help tailor online experiences for minors and keep them safer online, it is not a silver bullet. Age assurance is a complex topic that requires a delicate balancing of users' rights to safety, privacy, accuracy, and security.

[1] According to research on 'Mapping age assurance typologies and requirements', part of the Better Internet for Kids Strategy (BIK+) and available here, age assurance is the umbrella term for the methods that are used to determine the age or age range of an individual to varying lengths of confidence or certainty.

[2] Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available here.

[3] Directive (EU) 2018/1808 of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, available here.

Further, the online space offers a variety of services, only some of which hold risks of minors accessing them.

Therefore, any measures aiming to introduce age assurance should be proportionate to the risk profiles of the different online services. This in order to make sure that only those services that present the highest risk for minors are required to implement age-assurance methods. Such an approach would help minimise data collection and avoid undermining users' trust in and use of digital services, which are some of the risks that are commonly associated with age-assurance requirements.

Clearer guidelines and a measurable framework on how risks to minors are to be evaluated and which age-assurance methods are effective, proportionate, and appropriate to the risks would be helpful. Online services should also be afforded a certain degree of flexibility when determining which method to opt for and how to implement it. Because they need to do that in a way that is not only appropriate to the risk profile of their service, but also takes into account other considerations including economic feasibility, security, privacy expectations from users of the service, etc.

Given that there is no generally applicable solution that works for all services, collaboration among relevant industry players and public administrations, both at the national and European levels, is needed. With an internet ecosystem that continues to adapt to new trends and requirements, such as the need for interoperability between different services,[4] it will be necessary to develop solutions that work across the board, are easy to implement, scalable, and allow for seamless interoperability.

Likewise, users' trust in digital services is essential to the good functioning of the EU's Digital Single Market. That is why it's so important to make sure that any vetted solutions are adaptable and scalable, and help identify a user's age without divulging additional personal information.

II. Ensure uniform implementation of the European electronic identity framework

As the EU prepares for the full implementation of Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS Regulation),[5] the European Commission must provide clear guidelines for Member States on how to implement electronic identification means. This will prevent fragmentation and ensure interoperability across the European Union.

The eIDAS Regulation establishes a framework for European Digital Identity Wallets (EDIWs) that can be used for secure electronic identification and authentication across borders, without making it mandatory. Age assurance and hard-age verification (e.g. through governmental IDs) are complex topics and existing approaches present unique

[4] As mandated by Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), available here.

[5] Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, available here.

trade-offs in terms of accuracy, privacy, reliability, security, and liability, as concluded by the French Data Protection Authority among others.[6]

Based on this, establishing a unique electronic identification method across Europe could be a way forward. Whereas very large online platforms will be required under the eIDAS framework to accept and facilitate the use of EDIWs as a means to authenticate users,[7] all services need to be afforded legal certainty. In this context, and looking beyond very large online platforms, the Commission should explicitly recommend the use of eIDAS-compliant electronic identification means for age-verification purposes.

To guarantee EU-wide protection and uphold the Digital Single Market, however, it is essential to prevent fragmentation. In order for online services to rely on eIDAS-compliant methods, the Commission should ensure that these electronic identification means are interoperable across all EU Member States and fulfil the same requirements.

CCIA Europe believes that the Commission should work together with Member States to guarantee harmonised implementation that integrates privacy-enhancing technologies into EDIWs. This will ensure that parties relying on these systems are able to verify a user's age, without having to access or collect any additional categories of personal data. Any electronic identification means for age assurance must also necessarily comply with the privacy rules established by the General Data Protection Regulation (GDPR), including the principles of data minimisation, purpose limitation, data protection by design and by default, as well as with eIDAS requirements in terms of unobservability.

The Commission has launched a tender to develop an age-verification solution that is in line with the DSA and the Better Internet for Kids (BIK+) strategy. However, any work that is already underway should also ensure alignment with the eIDAS Regulation to develop an age-verification solution that is compatible with EDIWs. This is necessary to guarantee a high level of trust, security, and data protection for users of digital services in the EU. Furthermore, continued dialogue and collaboration with all industry players will be crucial to develop a streamlined and adaptable approach that can be deployed by all parties.

III. Provide transitional solutions that balance safety and privacy

While the eIDAS framework has the potential to complement existing age-assurance measures, its full implementation – and potential uptake – remain a work in progress. During this transition, online services must be able to rely on solutions that fulfil the same requirements for accuracy, security, and privacy protection for all users.

The eIDAS Regulation's digital wallets offer a promising way forward to consolidate age assurance. These wallets could securely store age credentials, allowing users to disclose only essential information while their privacy remains safeguarded. However, widespread adoption of these wallets may take time, and some users may be hesitant to use them, or simply do not want to own one.

[6] 'Online age verification: balancing privacy and the protection of minors', CNIL September 2022, available here.

[7] As stated in Article 5f(3) of Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, available here.

In the interim period, CCIA Europe believes transitional solutions that adequately balance safety and privacy concerns should be considered, namely:

- The extension of current digital wallets and credential infrastructure would offer practical and feasible ways to facilitate online age verification – minimising data collection and privacy risks for users, while maximising efficacy and user-friendliness.
    - The focus should be on developing and implementing a robust digital wallet age-assurance framework that provides achievable means of enhancing age assurance, and outlining a clear roadmap for its implementation.
- A platform-neutral framework could be implemented, containing assured age information that is stored in a digital wallet – whether private or governmental.
    - Providers of digital wallets could enable users to store age assurances in their wallets, including verification through official IDs, and to share assured-age signals with app developers as a way to access age-gated services.
    - In this case, both wallet providers and app developers should incorporate privacy-preserving technologies, including open-source zero-knowledge-proof technologies. Such a framework should be compatible with website integration and complement, rather than replace, existing age-assurance measures.

To guarantee an appropriate uptake, any wallet-based framework for age assurance should be in line with the existent EU-wide regulatory framework; but also harmonised and standardised, easy to adopt, scalable, and interoperable.

CCIA Europe notes with concern that some Member States are seeking to adopt – and are already implementing – diverging initiatives when it comes to age assurance and age-appropriate digital services. Given that providing minors a higher degree of protection is a goal shared by all, the way to do so should be through a common European approach that is developed collaboratively, and is adaptable to the different kinds of services available on the market, taking into account industry's best practices.

Indeed, CCIA Europe believes that the Commission, in collaboration with Member States and relevant national authorities, should be able to provide online service providers with a list of trusted partners (e.g. credential issuers) that can help drive this framework forward. This list could include open-source solutions, electronic identification platforms that are already in place in certain Member States, and other secure identity partners that are sufficiently vetted and trustworthy.

When developing any age-assurance solution, the Commission should ensure that the highest level of privacy, security, and trust is afforded, for example by integrating zero-knowledge proof protocols. This would allow the verification of users' age without revealing any unnecessary additional personal information about the user and guarantee an adequate and safe uptake, both by users and the industry.

Further, to help with uptake, Member States and the EU should launch awareness campaigns to inform citizens about the benefits and functionalities of publicly vetted electronic identification means. While younger generations are increasingly aware of the opportunities and risks that digital services present, it is also important for everyone in their environment to acquire robust knowledge when it comes to responsible use of online services. Therefore, such campaigns promoting awareness and media literacy should target not only minors but also parents, guardians, educators, and particularly vulnerable groups – all with a view to enhancing their digital literacy and empowering them to make informed choices.

Conclusion

The safety and well-being of minors on the internet is a collective responsibility that requires a collaborative approach. While age assurance could play a valuable role in creating a safer and more enriching online experience for young users, it can never serve as a standalone measure or isolated policy choice.

To properly ensure online safety, adequate policy frameworks are needed that uphold privacy, incorporate interoperable solutions, and embed safety by-design principles, all while leveraging industry-driven innovation. CCIA Europe and its Members remain committed to actively promoting safety, trust, and inclusivity within the digital ecosystem.

As the European Union continues to explore ways to enhance online protections – and while discussions on the best approaches to protecting minors online and providing age-appropriate services evolve – the importance of public-private collaboration becomes even more critical.

Public administrations, industry leaders, and civil society must come together to exchange best practices and develop scalable and adaptable solutions that are future-proof, provide robust safeguards for minors, and do not compromise user trust or digital inclusivity.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org