



Human Factors (HF); Age Verification Pre-Standardization Study Part 1: Stakeholder Requirements

Document Preview

[ETSI TR 104 077-1 V1.1.1 \(2024-09\)](https://standards.iteh.ai/catalog/standards/etsi/8bb76db5-36d8-4df5-a880-dab7fef27910/etsi-tr-104-077-1-v1-1-1-2024-09)

<https://standards.iteh.ai/catalog/standards/etsi/8bb76db5-36d8-4df5-a880-dab7fef27910/etsi-tr-104-077-1-v1-1-1-2024-09>

Reference

DTR/HF-00301567

Keywords

age verification, requirements, stakeholders

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI [Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Executive summary	5
Introduction	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	12
3.3 Abbreviations	12
4 Age Verification Overview	13
5 Stakeholders categorization.....	14
6 Age Verification sources	16
6.1 Method for analysing and collecting information	16
6.2 Information collected on Age verification and estimation	16
6.2.1 Introduction.....	16
6.2.2 Regulatory Guidance	17
6.2.2.1 France.....	17
6.2.2.1.1 CNIL - Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy (August 2021).....	17
6.2.2.1.2 CNIL - Online age verification: balancing privacy and the protection of minors (September 2022).....	19
6.2.2.2 Ireland	20
6.2.2.2.1 DPC - Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing (December 2021; see Chapter 5: Age of digital consent and age verification).....	20
6.2.2.3 Spain	22
6.2.2.3.1 AEPD - Decalogue of principles: Age verification and protection of minors from inappropriate content (December 2023).....	22
6.2.2.3.2 Draft Spanish law on the protection of children and adolescents in the digital environment.....	23
6.2.2.4 United Kingdom.....	25
6.2.2.4.1 ICO - Age assurance for the Children's code (January 2024).....	25
6.2.2.4.2 Ofcom - Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services: Annex 2 (December 2023).....	26
6.2.3 Standards and Certifications	27
6.2.3.1 BSI PAS 1296:2018 - Online age checking. Provision and use of online age check services. Code of Practice (March 2018)	27
6.2.3.2 IEEE 2089-2021 - IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children.....	28
6.2.3.3 IEEE 2089.1-2024 - IEEE Draft Standard for Online Age Verification	29
6.2.3.4 Age Check Certification Scheme	31
6.2.3.5 NIST - Face Analysis Technology Evaluation (FATE) Age Estimation & Verification	32
6.2.4 Age Assurance Projects	33
6.2.4.1 CNIL (France) - Demonstration of a privacy-preserving age verification process (June 2022)	33
6.2.4.2 AEPD (Spain) - Technical note - Description of the proofs on concept for systems for age verification and protection of minors from inappropriate content (December 2023).....	34
6.2.5 Resources - Government.....	35
6.2.5.1 Digital Regulation Cooperation Forum (UK) - Families' attitudes towards age assurance (October 2022)	35
6.2.5.2 Measurement of Age Assurance Technologies (2022).....	36

6.2.5.3	Measurement of Age Assurance Technologies - Part Two (August 2023)	36
6.2.5.4	Yoti Facial Age Estimation White Paper	37
6.2.6	Resources - Academia and Civil Society	38
6.2.6.1	5Rights Foundation - But how do they know it is a child? (October 2021)	38
6.2.6.2	The Center for Growth and Opportunity - Keeping Kids Safe Online: How Should Policymakers Approach Age Verification? (June 2023)	40
6.2.6.3	UNICEF - Digital Age Assurance Tools and Children's Rights Online across the Globe: A discussion paper (April 2021)	41
6.2.6.4	Praesidio Safeguarding - Making age assurance work for everyone: inclusion considerations for age assurance and children	42
6.2.7	Resources - Industry Think Tanks	44
6.2.7.1	The Age Verification Providers Association - Privacy; a foundational concept for age verification (March 2024)	44
6.2.7.2	Centre for Information Policy Leadership - Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable (March 2023)	45
6.2.7.3	Centre for Information Policy Leadership - A Multi-Stakeholder Dialogue on Age Assurance (March 2024)	46
6.2.7.4	Digital Trust & Safety Partnership - Age Assurance: Guiding Principles and Best Practices (September 2023)	47
6.2.7.5	euCONSENT / Simone van der Hof - Methods for Obtaining Parental Consent and Maintaining Children Rights (September 2021); Age assurance and age appropriate design: what is required? (November 2021)	49
6.2.7.6	Family Online Safety Institute - Making Sense of Age Assurance: Enabling Safer Online Experiences (November 2022)	52
6.2.7.7	Future of Privacy Forum - Unpacking Age Assurance: Technologies and Tradeoffs (June 2023)	53
6.2.7.8	Age Check Certification Scheme: Global Age Assurance Standards Summit 2024	54
7	Stakeholders requirements	55
7.0	Overview	55
7.1	Underage users of internet services and recipients of information groups requirements	55
7.2	Parents of underage users' requirements	57
7.3	Adult users of internet services and recipients of information groups requirements	58
7.4	Providers of age verification services and national authorities providing age verification solutions	59
7.5	Service/products providers subject to age verification obligations	60
8	Conclusions	61
History		62

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Human Factors (HF).

The present document is part 1 of a multi-part deliverable covering Age Verification Pre-Standardization Study, as identified below:

Part 1: "Stakeholder Requirements";

Part 2: "Solution and standards landscape";

Part 3: "Proposed Standardization Roadmap".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document outlines stakeholder requirements for age verification, essential for developing a standardized approach to age verification and age estimation solutions. The aim is to align efforts across various sectors and jurisdictions, ensuring the protection of minors online while complying with legal and regulatory requirements.

For underage users of internet services, the present document highlights the need for systems that reliably verify age using secure methods that protect personal data. It emphasizes the implementation of Privacy-Preserving verification methods to ensure anonymity and data minimization, collecting only the essential data necessary for age verification. The processes should be seamless, avoiding barriers for users.

Parents of underage users need systems that facilitate obtaining and verifying parental consent, ensuring both parents' involvement where applicable. The present document stresses transparency, providing clear, age-appropriate information about data collection and usage. Tools should allow parents to manage their children's online activities and revoke consent if necessary. Additionally, parents should be informed about safe online practices and the importance of privacy.

Adult users require assurances that any data collected during age verification will be protected and not misused. Clear information about the age verification process and data handling practices is essential for maintaining trust.

Providers of age verification services and national authorities have to adhere to GDPR [i.4], the Digital Services Act, and other relevant legal frameworks. The present document advocates for developing interoperable systems that work across various platforms and jurisdictions, implementing robust security measures to protect data during transmission and storage. Continuous oversight and updates to age verification methods are crucial to address emerging challenges.

Service providers subject to age verification obligations have to ensure the content provided is suitable for the verified age group. Compliance with national and international regulations regarding age-restricted content and services is mandatory. Age verification should not hinder user experience and be integrated smoothly into the service. Robust parental control settings should be integrated to manage access to content.

The plan for standardization involves establishing unified standards with comprehensive guidelines detailing the technical and procedural requirements for age verification systems. Encouraging the development of interoperable systems that can be easily adopted by service providers and verified by national authorities is important. Compliance with GDPR [i.4], eIDAS2 [i.2], and other relevant laws provides a legal framework for data protection and user privacy. Regular audits and compliance checks help maintain the integrity of age verification processes.

Collaboration among stakeholders, including service providers, regulatory bodies, parents, and user advocacy groups, ensures solutions meet diverse needs and concerns. Educational campaigns inform stakeholders about the importance of age verification and effective tool usage. Establishing feedback mechanisms to gather input from stakeholders, staying updated with technological advancements, and incorporating innovative solutions to address new challenges are essential steps.

(<https://standards.iteh.ai>)

Introduction

Document Preview

The present document aims to establish and analyse stakeholder requirements for age verification, laying the groundwork for future European standards in this field as requested in the Digital Services Act. Regulation (EU) 2022/2065 [i.1] mandates the development of standards for targeted measures to protect minors online (Article 44 (j)), including age verification systems and parental control tools (Article 35 (j)). However, achieving a unified European solution for age verification might be challenging due to disparate national systems. Thus, establishing comprehensive requirements for age verification and parental controls, as well as standardized interfaces for service providers to access verified age data, is crucial for protecting minors online. International organizations like ITU/IEC, national standards bodies, and the euConsent EU-funded project have explored age verification and protection of minors. Their research provides a basis for assessing current solutions and identifying gaps.

While the euConsent project explored age verification in depth, its solutions primarily focus on agency-supported verification, leaving significant questions unanswered. Specifically, the seamless sharing of verified age data among parents, minors, and service providers remains underexplored.

The present document will focus on identifying and understanding the requirements of all stakeholders with an interest in age verification. The present document aims at understanding the needs of different stakeholder groups, including children, parents, service providers, and society as a whole, in their use of age-verified information, and to define the requirements of stakeholders comprehensively, ensuring future standards are practical and meet the needs of all parties involved.

1 Scope

The present document identifies stakeholder requirements for age verification.

NOTE: The present document may assist in providing the groundwork for defining standards as outlined in the Digital Services Act [i.1]. Its purpose is to establish the foundation for developing European standards in age verification and protecting minors online.

The present document presents the analysis of requirements of identified stakeholders in the age verification process for whom accurate age information is essential to their service access or to their business operation.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

- [i.1] [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
- [i.2] [Regulation \(EU\) 2024/1183](#) of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- [i.3] [Regulation \(EU\) No 910/2014](#) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- [i.4] [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- [i.5] ETSI TS 119 461 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".
- [i.6] ISO/IEC WD 27566-1: "Information security, cybersecurity and privacy protection Age assurance systems. Framework Part 1: Framework".
- [i.7] [UNICEF](#): "Convention on the Rights of the Child".
- [i.8] [OFCOM](#): "Quick guide to children's access assessments".
- [i.9] [OFCOM](#): "Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online service".
- [i.10] [CNIL - Recommendation 7](#): "Check the age of the child and parental consent while respecting the child's privacy". (August 2021).

- [i.11] [CNIL - Online age verification](#): "Balancing privacy and the protection of minors". (September 2022).
- [i.12] [DPC - Front and Centre](#): "Fundamentals for a Child-Oriented Approach to Data Processing". (December 2021).
- [i.13] [AEPD - Decalogue of principles](#): "Age verification and protection of minors from inappropriate content". (December 2023).
- [i.14] Draft Spanish law on the protection of children and adolescents in the digital environment.
- [i.15] [ICO](#): "Age assurance for the Children's code". (January 2024).
- [i.16] [BSI PAS 1296:2018](#): "Online age checking; Provision and use of online age check services; Code of Practice (March 2018)".
- [i.17] IEEE 2089™-2021: "IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children".
- [i.18] IEEE 2089.1™-2024: "IEEE Draft Standard for Online Age Verification".
- [i.19] NIST: ["Face Analysis Technology Evaluation \(FATE\) Age Estimation & Verification"](#).
- [i.20] CNIL: "Demonstration of a privacy-preserving age verification process". (June 2022).
- [i.21] AEPD: "Technical note - Description of the proofs on concept for systems for age verification and protection of minors from inappropriate content". (December 2023).
- [i.22] Digital Regulation Cooperation Forum (UK): "Families' attitudes towards age assurance". (October 2022).
- [i.23] [Measurement of Age Assurance Technologies - Part Two \(August 2023\)](#): "Measurement of Age Assurance Technologies. A Research Report for the Information Commissioner's Office (ICO)".
- [i.24] [Yoti](#): "Facial Age Estimation White Paper".
- [i.25] [5Rights Foundation](#): "But how do they know it is a child?" (October 2021).
- [i.26] [The Center for Growth and Opportunity](#): "Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?" (June 2023).
- [i.27] [UNICEF](#): "Digital Age Assurance Tools and Children's Rights Online across the Globe: A discussion paper". (April 2021).
- [i.28] Praesidio Safeguarding: "Making age assurance work for everyone: inclusion considerations for age assurance and children".
- [i.29] The Age Verification Providers Association: "Privacy; a foundational concept for age verification". (March 2024).
- [i.30] [Centre for Information Policy Leadership](#): "Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable". (March 2023).
- [i.31] [Centre for Information Policy Leadership](#): "A Multi-Stakeholder Dialogue on Age Assurance". (March 2024).
- [i.32] Digital Trust & Safety Partnership: "Age Assurance: Guiding Principles and Best Practices". (September 2023).
- [i.33] euCONSENT / Simone van der Hof: "Methods for Obtaining Parental Consent and Maintaining Children Rights". (September 2021); "Age assurance and age appropriate design: what is required?". (November 2021).
- [i.34] [Family Online Safety Institute](#): "Making Sense of Age Assurance: Enabling Safer Online Experiences". (November 2022).
- [i.35] Future of Privacy Forum: "Unpacking Age Assurance: Technologies and Tradeoffs". (June 2023).

- [i.36] 36Age Check Certification Scheme: "Global Age Assurance Standards". Summit 2024.
- [i.37] UK: "[Online Safety Act 2023](#)".
- [i.38] [Regulation \(EC\) No 765/2008](#) of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93.
- [i.39] United Nations Convention on the Rights of the Child (UNCRC), 1989.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

age: length of time that a person or thing has existed

age assurance: methods used to determine the age or age range of an individual, including age verification, estimation, and self-declaration

age check exchange: online gateway where age check providers and parties assess user attributes

NOTE: See PAS 1296:2018 [i.16].

age check provider: organization responsible for establishing and maintaining a person's identity attributes

NOTE: See PAS 1296:2018 [i.16].

age estimation: process to determine an individual's likely age range by analysing inherent features or behaviours

age gate: technical measure that restricts access to digital content for those who are not of the appropriate age

Age Verification (AV): process to determine an individual's age or age range

attestation of attributes validation: process of verifying and confirming that an attestation of attributes is valid

NOTE: See eIDAS2 definition [i.2].

attribute: characteristic, quality, right or permission of a natural person

NOTE: See eIDAS2 definition [i.2].

authentication: electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form

NOTE: See eIDAS2 definition [i.2].

authentic source: repository or system, held under the responsibility of a public sector body or private entity, which contains and provides attributes about a natural and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

NOTE: See eIDAS2 definition [i.2].

child: natural person under 18 years of age

children's rights: rights as outlined in the United Nations Convention on the Rights of the Child (UNCRC) [i.39], focusing on ensuring child welfare and protection

conformity assessment body: entity as defined in Article 2, point 13, of Regulation (EC) No 765/2008 [i.38], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a service provider and the services it provides

consent: clear and informed indication that a data subject agrees to data processing

contra-indicator: information that contradicts a claimed age attribute or identity, raising doubts about its validity

digital identity document: identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form

NOTE 1: Machine-processable, in this case, does not include optical scanning and processing of a physical identity document.

NOTE 2: A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.

NOTE 3: The "electronic identification" part of a passport or national identity card is sometimes called "electronic identity" or even "eID". In the present document, this part of a passport or national identity card is a digital identity document.

electronic attestation of attributes: attestation in electronic form that allows the authentication of attributes describing features, characteristics or qualities of a natural or legal person or of an entity, or a natural person representing a legal person, or of an object

NOTE: See eIDAS2 definition [i.2].

electronic identification: process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person

NOTE: See eIDAS2 definition [i.2].

electronic Identification means (eID means): material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service

NOTE: See eIDAS2 definition [i.2].

eID scheme: governance model and technical specifications allowing interoperability between eID means from different eID providers

(identity) evidence: information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct

NOTE: See ETSI TS 119 461 [i.5].

identity: attribute or set of attributes that uniquely identify a person within a given context

NOTE: See ETSI TS 119 461 [i.5].

identity matching/identification: process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person

NOTE: See ETSI TS 119 461 [i.5].

identity proofing context: external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself

NOTE: See ETSI TS 119 461 [i.5].

identity proofing (process): process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes

NOTE: See ETSI TS 119 461 [i.5].

indicators of confidence: quantitative, qualitative or descriptive measure of the correctness and accuracy to which an age assurance attribute can be stated to relate to a natural person

NOTE: See ISO 27566-1 (Committee Draft) [i.6].

legitimate evidence holder: person for whom the evidence is issued

NOTE: See ETSI TS 119 461 [i.5].

Level of Identity Proofing (LoIP): confidence achieved in the identity proofing

liveness detection: measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture

parental consent: consent from someone with parental authority over children under a specified age

parental controls: filtering settings to monitor children's online activity and protect them from harmful content

personal data: any information as defined in Article 4, point (1), of Regulation (EU) 2016/679 [i.4]

physical identity document: identity document issued in physical and human-readable form

EXAMPLE: The printed (non-digital) representation of passport.

NOTE: See ETSI TS 119 461 [i.5].

profiling: automated processing of personal data to evaluate personal aspects like work performance or behaviour

pseudonym: fictitious identity that a person assumes for a particular purpose, which differs from their original or true identity

NOTE 1: Pseudonym identity can, as opposed to an anonymous identity, be linked to the person's real identity.

NOTE 2: See ETSI TS 119 461 [i.5].

pseudonymization: process of processing data in a way that cannot be attributed to an individual without additional information

relying party: natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service on an age assurance assertion or claim to make an age-related eligibility decision

NOTE: See eIDAS2 definition [i.2].

remote identity proofing: identity proofing process where the applicant is physically distant from the location of the identity proofing

NOTE: See ETSI TS 119 461 [i.5].

selective disclosure: capability of the application that enables the user to present a subset of attributes

EXAMPLE: EUDI Wallet and an Electronic Attestation of Attributes (EAA) with the attributes first name, last name, birth date, and address. The user can for example selectively disclose only its first name.

strong user authentication: authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inference, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

NOTE: See eIDAS2 definition [i.2].

unique identifier: unique data used to represent a person's identity and associated attributes

unlinkability: lack of information required to connect the user's selectively disclosed attributes beyond what is disclosed

NOTE 1: Verifier unlinkable means that one or more verifiers cannot collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 2: Issuer unlinkable means that one or more issuers cannot collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 3: Fully unlinkable means that no party can collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 4: Multi-show unlinkability means that a (Q)EAA can be used for multiple presentations, which cannot be used to connect the user's selectively disclosed attributes.

NOTE 5: The opposite of multi-show unlinkability means that, i.e. a (Q)EAA can only be used once for a presentation, since the (Q)EAA will thereafter reveal information that can be used for linkability.

untraceability: property that ensures that an age assurance attribute used by a natural person in a particular context cannot be traced to that natural person by a relying party

NOTE: Untraceability applies to other third parties not being able to trace back to the age assurance service provider, but individuals would be aware of the age assurance service provider to be able to exercise their data rights.

validation: part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid

Zero-Knowledge Proof (ZKP): method by which the user (prover) can prove to the relying party (verifier) that a given statement is true while the user does not provide any additional information apart from the fact that the statement is true

NOTE 1: There are special-purpose ZKPs that can only prove very specific statements (knowledge of a pre-image of a hash or knowledge of a signature under a specific digital signature scheme) and general-purpose or programmable ZKPs that allow to prove any statement. Programmable ZKPs usually involve a compiler from some programming language that describes the statement to be proved (program returns a certain public value upon correct execution on a private input) into a ZKP proving and verification program.

NOTE 2: A ZKP protocol should meet the following three criteria: Completeness (if the statement is true then a user can convince a verifier), soundness (a fraudulent user cannot convince a verifier of a false statement beyond negligible probability - how small is a parameter choice, 2^{-128}), and zero-knowledge (the interaction only reveals if a statement is true and nothing else beyond what can trivially be inferred from the statement itself).

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AE	Age Estimation
AEPD	Agencia Española de Protección de Datos
AI	Artificial Intelligence
AV	Age Verification
CCPA	California Consumer Privacy Act
CIPL	Centre for Information Policy Leadership
CNIL	Commission Nationale de l'Informatique et des Libertés
COPPA	Children's Online Privacy Protection Act
CRIA	Children's Rights Impact Assessment
DPC	Data Protection Commission
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EAA	Electronic Attestation of Attributes
EDPB	European Data Protection Board
EEE	Institute of Electrical and Electronics Engineers
eID	electronic Identification
eIDAS	electronic Identification, Authentication and Trust Services
eMRTD	electronic Machine-Readable Travel Document
EUDI	European Digital Identity
FOSI	Family Online Safety Institute
FPR	False Positive Rate
FTC	Federal Trade Commission

ICO	Information Commissioner's Office
ISO	International Standards Organisation
ISS	Information Society Services
LO	Ley Orgánica
LoIP	Level of Identity Proofing
MAE	Mean Absolute Error
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
PAS	Publicly Available Specification
QEAA	Qualified Electronic Attestation of Attributes
QR	Quick Response
TPR	True Positive Rate
UKAS	United Kingdom Accreditation Service
UNCRC	United Nations Convention on the Rights of the Child
URL	Uniform Resource Locator
VoCO	Voice Controlled Operations
VPN	Virtual Private Network
ZKP	Zero-Knowledge Proof

4 Age Verification Overview

Age assurance is required across a wide range of online industry sectors. There are guides being made available by government organizations to aid online industries in ensuring they are complying to regulations. Ideally, the online industries keep risks and safety measures under regular review.

For example:

- Betting and Gambling
- Music Streaming Sites
- Video Sharing Platforms
- Adult websites
- Advertising platforms
- Social Media
- Computer Gaming
- Online Pharmacies
- Knives and acid sales
- Cannabinoid sales
- Supermarkets
- Fast food delivery
- Vaping sites
- Dating sites

These requirements arise for a number of common reasons:

- 1) Child Protection e.g. risk management when adults interact with children online;
- 2) Data Protection e.g. to implement Article 8, GDPR [i.4];
- 3) Age-restricted products e.g. vaping, alcohol;

- 4) Age-restricted services e.g. gambling;
- 5) Age-restricted content e.g. pornography, violent games.

Table 1

	Child Protection	Data Protection	Age-restricted products	Age-restricted services	Age-restricted content
Betting and Gambling		X		X	
Music Streaming Sites					
Video Sharing Platforms	X	X			X
Adult websites	X	X			X
Advertising platforms		X	X		
Social Media	X	X		X	X
Computer Gaming	X	X			
Online Pharmacies		X	X		
Knives and acid sales		X	X		
Cannabinoid sales		X	X		
Supermarkets		X	X		
Fast food delivery		X	X		
Vaping sites		X	X		
Dating sites	X	X		X	X

5 Stakeholders categorization

At its broadest, the stakeholders in this process will include almost everyone who makes use of the internet. However, some stakeholders will require particular attention and will be the principal target of the present document. It should be noted that there is guidance available to aid specific industries to enable them to comply age verification regulations., though these are often by specific national laws. Amongst these stakeholders, the following ones have been identified:

- Underage users of internet services and recipients of information groups.
- Parents of underage users.
- Adult users of internet services and recipients of information groups.
- Providers of age verification services and national authorities providing age verification solutions.
- Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.

The stakeholders will have one or more of the following requirements covered:

- **Accurate age attribution:** Age verification systems are needed to attribute correct age information to children, using reliable identification.
- **Adequate content delivery:** Use accurate age information to provide appropriate content/services to minors as set by parents or law.
- **Age-appropriate content:** Ensure that information and services accessible to underage users are suitable for their age group.
- **Compliance:** Ensure solutions comply with national and international regulations, such as the EU Digital Services Act [i.1], UK Online Safety Act [i.37] and eIDAS2 [i.2].