ETSI TR 104 077-2 V1.1.1 (2024-12)

Human Factors (HF);
Age Verification Pre-Standardization Study
Part 2: Solutions and Standards Landscape

Reference
DTR/HF-00301568

Keywords
age verification, privacy, security, user

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 repository.

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

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 2 of a multi-part deliverable covering Age Verification Pre-Standardization Study, as identified below:

Part 1: "Stakeholder Requirements";

Part 2: "Solutions 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 reviews and analyses existing solutions and standards for age verification in Europe: technological solutions; national/regional implementations and regulations, and existing standardization (IEC, others, etc.). The range of technical solutions and existing implementations (national and regional) is reviewed from the perspective of the stakeholders' requirements identified in ETSI TR 104 077-1 [i.7].

Introduction

The present document aims to identify the existing solutions and standards landscape for age verification, laying the groundwork for future European standards in this field as requested in the Digital Services Act. A heterogeneous landscape of age-verification solutions exists from "Click here to confirm that you are 18 years old or older" to sophisticated technical solutions involving the verification of official documents (machine-readable ID cards). Regulation (EU) 2022/2065 [i.51] 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 a comprehensive understanding of the landscape 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/ISO/IEEE, national standards bodies, and the euConsent NGO 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, with follow-on projects for age verification exploring unanswered questions. For example, the direct sharing of verified age data between parents, minors, and digital service providers without the need for third-party age assurance providers is an area that requires further study.

The present document will focus on identifying and understanding the existing and proposed solutions plus the standards landscape in age verification. The present document aims to understand how the existing solutions and standards can be used to meet the stakeholder requirements for age verification as identified in ETSI TR 104 077-1 [i.7], this includes standards and solutions that are not specifically aimed at age verification as many of the stakeholder requirements are the same as other cybersecurity, privacy and data protection requirements found throughout many different industries and services.

1 Scope

The present document reviewed from a perspective of the stakeholder requirements identified in ETSI TR 104 077-1 [i.7] is a study of the landscape of international, regional and national existing solutions (identified in ETSI TR 104 077-1 [i.7]), approaches (frameworks/architecture) and standards for age verification in Europe.

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] ETSI TR 103 305-1 (V4.1.2) (2022-04): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.2] ETSI TR 103 305-2 (V2.1.1) (2018-09): "CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing".

[i.3] ETSI TR 103 305-4 (V3.1.1) (2022-11): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.4] ETSI TR 103 305-5 (V2.1.1) (2023-02): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.5] ETSI TR 103 935 (V1.1.1) (2023-12): "Cyber Security (CYBER); Assessment of cyber risk based on products' properties to support market placement".

[i.6] ETSI TS 103 457 (V1.2.1) (2023-03): "CYBER; Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain".

[i.7] ETSI TR 104 077-1: "Human Factors (HF); Age Verification Pre-Standardization Study; Part 1: Stakeholder Requirements".

[i.8] ETSI TR 103 370 (V1.1.1) (2019-01): "Practical introductory guide to Technical Standards for Privacy".

[i.9] ETSI TS 103 485 (V1.1.1) (2020-08): "CYBER; Mechanisms for privacy assurance and verification".

[i.10] ETSI TR 103 642 (V1.1.1) (2018-10): "CYBER; Security techniques for protecting software in a white box model".

[i.11] ETSI TR 103 309 (V1.1.1) (2015-08): "CYBER; Secure by Default - platform security technology".

[i.12] ETSI TS 102 165-1 (V5.2.5) (2022-01): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.13] ETSI TS 103 992 (V1.1.1) (2024-05): "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.14] ETSI TR 103 838 (V1.1.1) (2022-01): "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.15] ETSI EG 203 499 (V3.1.1) (2024-07): "Human Factors (HF); User-centred terminology for existing and upcoming ICT devices, services and applications".

[i.16] ETSI EN 301 549 (V3.2.1) (2021-03): "Accessibility requirements for ICT products and services".

[i.17] ETSI TR 103 349 (V1.1.1) (2016-12): "Human Factors (HF); Functional needs of people with cognitive disabilities when using mobile ICT devices for an improved user experience in mobile ICT devices".

[i.18] ETSI EG 203 350 (V1.1.1) (2016-11): "Human Factors (HF); Guidelines for the design of mobile ICT devices and their related applications for people with cognitive disabilities".

[i.19] IEEE 2089™-2021: "IEEE Standard for an Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children".

[i.20] IEEE P2089.2™: "IEEE Standard for Terms and Conditions for Children's Online Engagement".

[i.21] IEEE 2089.1™-2024: "IEEE Standard for Online Age Verification".

[i.22] CNIL (2022): "Demonstration of a privacy-preserving age verification process".

[i.23] Agcom (2024): "Linee guida parental control (Delibera n. 9/23/CONS)".

[i.24] Coimisiún na Meán (2024): "Online Safety Code".

[i.25] AEDPD (2023): "Decalogue of principles - Age verification and protection of minors from inappropriate content".

[i.26] KJM (2022): "Criteria for evaluating concepts for age verification systems as elements for ensuring closed user groups in telemedia in accordance with § 4 para. 2 sentence 2 Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia (JMStV) ("AVS-MATRIX")".

[i.27] ICO: "Age appropriate design: a code of practice for online services".

[i.28] ICO: "Age assurance for the Children's code".

[i.29] Ofcom (2023): "Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services".

[i.30] Ofcom (2024): "Quick guide to children's access assessments".

[i.31] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (Text with EEA relevance).

[i.32] CEN and CENELEC Workshop Agreement (2023) CWA 18016: "Age appropriate digital services framework".

[i.33] ISO/IEC DIS 27566-1: "Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework".

[i.34] ISO/IEC PWI 27566-2 (Ed 2): "Age assurance systems — Part 2: Technical approaches and guidance for implementation".

[i.35] ISO/IEC AWI 27566-3 (Ed 3): "Age assurance systems — Part 3: Benchmarks for benchmarking analysis".

[i.36] ITU (2020): "Digiworld An example of how the ITU Guidelines on Child Online Protection can be delivered in practice".

[i.37] Ministry for the Digital Transformation and Civil Service (2024): "Digital Wallet; Specification for the use of the "Age of majority" credential Age verification system for access to online content".

[i.38] Ministry for the Digital Transformation and Civil Service (2024): "Digital Wallet; Age verification protocol Age verification system for access to online content".

[i.39] ISO/IEC JTC 1/SC 27 TR 15443-1:2012: "Information technology — Security techniques — Security assurance framework Part 1: Introduction and concepts".

[i.40] ISO/IEC JTC 1/SC 27 TR 15443-2:2012: "Information technology — Security techniques — Security assurance framework Part 2: Analysis".

[i.41] ISO/IEC JTC 1/SC 27 29115:2013: "Information technology — Security techniques — Entity authentication assurance framework".

[i.42] ISO/IEC JTC 1/SC 27 29128-1:2023: "Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework".

[i.43] ISO/IEC JTC 1/SC 27 27551:2021: "Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication".

[i.44] ISO/IEC JTC 1/SC 37; 30136:2018: "Information technology — Performance testing of biometric template protection schemes".

[i.45] ISO/IEC JTC 1/SC 37; 24714:2023: "Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance".

[i.46] ISO/IEC JTC 1/SC 37; TR 30110:2015: "Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children".

[i.47] AgeAware; euConsent (2024), AgeAware® Specification, Consultation Document: "WP1: Business Requirements".

[i.48] Produced by Childnet International for The National Lottery Heritage Fund, Digital Skills for Heritage: "Working with Children and Young People Online".

[i.49] NCSC: "Cyber Essentials".

[i.50] BSI PAS 1296:2018: "Online age checking. Provision and use of online age check services. Code of Practice".

[i.51] 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.52] 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.53] ETSI TS 119 461 (V1.1.1) (2021-07): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.54] ETSI TS 119 462: "Electronic Signatures and Trust Infrastructures (ESI); Wallet interfaces for trust services and signing".

[i.55] ETSI TS 119 471: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attribute Services".

[i.56] ETSI TS 119 475: "Electronic Signatures and Trust Infrastructures (ESI); Relying party authorizations for access to EUDI Wallet".

[i.57] ETSI EN 319 411-2 (V2.5.1) (2023-10): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.58] IEEE 2089.3™: "Online Parental Consent".

[i.59] ETSI TR 104 077-3: "Human Factors (HF); Age Verification Pre-Standardization Study; Part 3: Proposed Standardization Roadmap".

[i.60] ETSI TR 104 031 (V1.1.1) (2024-01): "Securing Artificial Intelligence (SAI); Collaborative Artificial Intelligence".

[i.61] ETSI TR 104 032 (V1.1.1) (2024-02): "Securing Artificial Intelligence (SAI); Traceability of AI Models".

[i.62] ETSI TR 104 225 (V1.1.1) (2024-04): "Securing Artificial Intelligence TC (SAI); Privacy aspects of AI/ML systems".

[i.63] ETSI TR 104 048: "Securing Artificial Intelligence; Data Supply Chain Security".

[i.64] ETSI TR 104 221: "Securing Artificial Intelligence; Problem statement".

[i.65] ETSI TR 104 062 (V1.2.1) (2024-07): "Securing Artificial Intelligence; Automated Manipulation of Multimedia Identity Representations".

[i.66] ETSI TS 104 223: "Securing Artificial Intelligence TC (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

[i.67] ETSI TS 104 224: "Securing Artificial Intelligence TC (SAI); Explicability and transparency of AI processing".

[i.68] Regulation (EU) 2022/2480 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 1025/2012 as regards decisions of European standardisation organisations concerning European standards and European standardisation deliverables.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

NOTE: From ISO 27566-1 [i.33]: "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".

age estimation: age assurance method-based analysis of biological or behavioural features of humans that vary with age

age inference: age assurance method based on verified information which indirectly implies that an individual is over or under a certain age or within an age range

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

NOTE: From ISO 27566-1 [i.33]: "age assurance method based on calculating the difference between a verified year or date of birth of an individual and a subsequent date". Also, in some cultures, an alternate calculation (such as use of birth year rather than birth date) may be applicable.

inclusivity: capability of a product to be utilized by people of various backgrounds include (and are not limited to) people of various ages, abilities, cultures, ethnicities, languages, genders, economic situations, education, geographical locations and life situations

practice statement: documentation of the practices, procedures and controls employed by an organization to fulfil a service

relying party: entity that relies on an age assurance result to make an age-related eligibility decision

3.2 Symbols

Void.

3.3 Abbreviations

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

ABUEA	Attribute-Based Unlinkable Entity Authentication
AENOR	Asociación Española de Normalización y Certificación
AEPD	Agencia Española de Protección de Datos
AFNOR	Association Française de Normalisation
Agcom	Communications Regulatory Authority
AI	Artificial Intelligence
AIA	AI Agents
AV	Age Verification
BSI	British Standards Institution
CCPN	Standardization Coordination and Steering Committee
CEI	Comitato Elettrotecnico Italiano
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIA	Confidentiality, Integrity, Availability
CNIL	Commission nationale de l'informatique et des libertés
COP	Child Online Protection
COS	Strategic Committees
CSC	Critical Security Control
DID	Decentralized Identifier
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
DNE	Digital Networked Economy
EG	ETSI Guide
EN	European Standard
ESI	Electronic Signatures and Trust Infrastructures
ESO	European Standard Organisation
ETSI	European Telecommunications Standards Institute
EUDI	European Digital Identity
GDPR	General Data Protection Regulation
HF	Human Factors
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISS	Internet Society Services
ITU	International Telecommunication Union
JMStV	Interstate Treaty on the Protection of Minors in the Media
KJM	Kommission für Jugendmedienschutz
LoA	Levels of Entity Authentication
NCSC	National Cyber Security Centre
NIS2	Revised Network and Information Security Directive
NSAI	National Standards Authority of Ireland
NSB	National Standards Bodies
PAS	Publicly Available Specification
SAI	Securing Artificial Intelligence
SDO	Standards Development Organization
TC	Technical Committee

TR	Technical Report
TS	Technical Specification
UNI	Ente Nazionale Italiano di Unificazione
WBC	White Box Cryptography

4 Overview and Diagram of Age Assurance Systems

4.1 Overview

Age-related eligibility decisions are required when a person should either be a certain age, older or younger than a given age or be within an age range, where ages are counted in years and where these criteria are dependent upon the type of goods, content, services, venues or spaces to be provided. Although an individual's age is an attribute of their identity, it is not necessarily the case that establishing the full identity of an individual in a global context is needed to gain age assurance. As such, the process of age assurance may in some instances be connected to identity verification but can also be performed in ways other than via identity verification.

An age assurance system should be capable of meeting the stated and implied needs of relying parties when it is used under specified conditions. A functionally complete age assurance system comprises of one or more age assurance methods selected or designed to provide the relying party with the necessary information to make an age-related eligibility decision. The functional characteristics (performance, privacy, security and acceptability) describe what a relying party, intermediary or age assurance provider is supposed to accomplish as set out in their practice statement.

4.2 Diagrams

Both figures 1 and 2 are from ISO/IEC DIS 27566-1:2025 [i.33].

Age assurance methods		
Age verification methods	**Age estimation methods**	**Age inference methods**
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

Figure 1: Illustration of the three age assurance methods

Figure 1 describes the three different age assurance methods, which when taken together with the binding of evidence to the individual can be used to generate an age assurance result leading to an age-related eligibility decision.

Figure 2 shows the different characteristics of an age assurance system with examples of standards, solutions and frameworks from clauses 5 and 6 that align with the different characteristics.

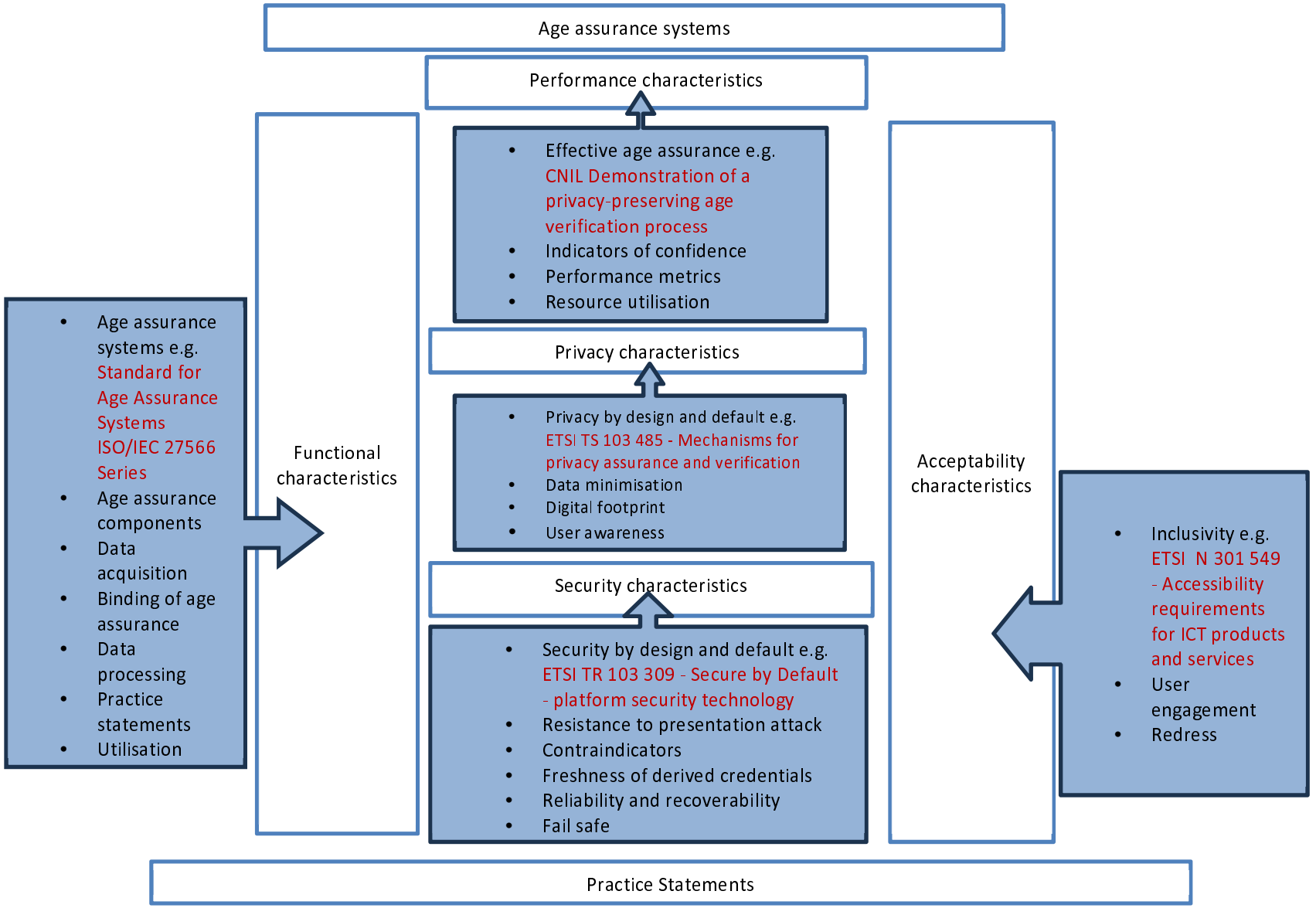

Figure 2: Illustration of the structure of the framework with example standards & solutions

5 Overview of European and International solutions and standards for Age Verification

5.1 Introduction

In this clause solutions and standards from regional and international standards development organizations will be identified and mapped to the relevant stakeholders' requirements from clause 7 of ETSI TR 104 077 [i.7] and copied to annex A.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardization [i.31] lays down a procedure for the provision of information in the field of technical standards and regulations and identifies the three European Standardization bodies responsible for drafting harmonised standards are European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI). Recently, Regulation (EU) No 2022/2480 [i.68] - adopted by the co-legislators on 14 December 2022 - introducing amendments to Regulation (EU) No 1025/2012 [i.31] to grant the decision-making on European Standards and European standardization deliverables to the National Standards Bodies (NSB).

5.2 Standards Development Organizations

5.2.1 ETSI

5.2.1.1 TC Cyber

The main responsibilities of ETSI TC CYBER are:

- To act as the ETSI centre of expertise in the area of Cyber Security.
- To advise and assist all ETSI Groups with the development of Cyber Security requirements.
- To develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI.
- To collect and specify Cyber Security requirements from relevant stakeholders.
- To identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects.
- To ensure that appropriate Standards are developed within ETSI in order to meet these requirements.
- To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects.
- To coordinate work in ETSI with external groups such as ENISA.
- To answer policy requests related to Cyber Security, and security in broad sense in the ICT sector.

The activities of TC CYBER are performed in close co-operation with relevant standards activities within and outside ETSI. They include the following broad areas:

- Cyber Security.
- Security of infrastructures, devices, services and protocols.
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators.
- Security tools and techniques.

- Provision of security mechanisms to protect privacy.
- Creation of security specifications and alignment with work done in other TCs.

Table 1: Mapping of ETSI TC CYBER output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
ETSI TS 103 992 - Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls [i.13]	It describes an ensemble of cybersecurity specifications and other materials, especially the ETSI Critical Security Controls in ETSI TR 103 305-1 [i.1] that can be applied to support NIS2 Directive requirements by EU Member States and affected essential and important entities. The present document also considers, and refers to, the work being done by ETSI ESI on Trust Services.	Privacy and Data protection Compliance and governance Implementation and governance
ETSI TR 103 305-1 - Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls [i.1]	It describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber-attacks. The measures reflect the combined knowledge of actual attacks and effective defences.	Privacy and Data protection Compliance and governance Implementation and governance
ETSI TR 103 305-2 - Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing [i.2]	This is a repository for measurement and effectiveness tests of Critical Security Control (CSC) implementations. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber-attacks.	Privacy and Data protection Compliance and governance Implementation and governance
ETSI TR 103 305-4 - Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms [i.3]	This is a repository for diverse facilitation mechanism guidelines for Critical Security Control implementations.	Privacy and Data protection Compliance and governance Implementation and governance
ETSI TR 103 305-5 - Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement [i.4]	This is a repository for data protection and privacy enhancing implementations using the Critical Security Controls, ETSI TR 103 305-1 [i.1]. These presently include a comprehensive, consistent approach for analysing the latest version of the Controls aiming to meet requirements that include the EU General Data Protection Regulation (GDPR) and the U.S. DHS Fair Information Practice Principles.	Privacy and Data protection Compliance and governance Implementation and governance
ETSI TR 103 935 - Assessment of cyber risk based on products' properties to support market placement [i.5]	The TR examines the background to the assessment of cybersecurity risks and identifies issues that may arise in the context of placing ICT products and services in the EU Single Market under the applicable legal requirements.	Implementation and Compliance Implementation and best practices
ETSI TS 103 457 - Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain [i.6]	The TS specifies a high-level service-oriented interface, as an application layer with a set of mandatory functions, to access secured services provided by, and executed in a More Trusted Domain. The transport layer is out of scope and left to the architecture implementation.	Privacy and Data Protection Implementation and best practices

Title of the Standard	Description	Stakeholder Requirement See Annex A
ETSI TR 103 838 - Guide to Coordinated Vulnerability Disclosure [i.14]	The TR is for companies and organizations of all sizes who want to implement a vulnerability disclosure process. It is not intended to be a comprehensive guide to creating and implementing a vulnerability disclosure process, but instead focuses on the essential steps. It contains generic advice on how to respond to and manage a vulnerability disclosure, a defined triage process, advice on managing vulnerabilities in third party products or suppliers, and an example vulnerability disclosure policy.	Privacy and data protection - data security Compliance and governance
ETSI TR 103 370 - Practical introductory guide to Technical Standards for Privacy [i.8]	The TR gives a guide to the use of standards to assist in the management of privacy.	Privacy and data protection Privacy by Design
ETSI TS 103 485 - Mechanisms for privacy assurance and verification [i.9]	The TS defines the means to enable assurance of privacy, using the conventional Confidentiality, Integrity, Availability (CIA) paradigm and with reference to the functional capabilities for privacy protection described in Common Criteria for Information Technology Security Evaluation. The mechanisms defined in the present document have been informed by the requirements found in articles and recitals of the General Data Protection Regulation (EU) 2016/679 (GDPR) [i.52] and can be considered in assisting in achieving compliance to the requirements in GDPR.	Privacy and data protection Privacy by Design Compliance - GDPR
ETSI TR 103 642 - Security techniques for protecting software in a white box model [i.10]	The TR reports on the application of techniques for protecting software implementations, in the form of applications and content, using software resident security techniques. It makes recommendations for the application of specific techniques including White Box Cryptography (WBC), code obfuscation, and other techniques denoted as anti-xxx and including anti-tampering, anti-reversing, anti-debugging, anti-cloning, etc. These techniques address the threats presented by attackers of the forms outlined in the document.	Data Security Implementation and best practices Enhanced security
ETSI TR 103 309 - Secure by Default - platform security technology [i.11]	This document is intended to encourage development and adoption of 'secure by default' platform security technologies by showing how they can be used to effectively solve real business problems and improve the usability of secure services. The intended audience is decision makers rather than engineering teams where they are deciding which features to include in a new platform, or which are required as part of a procurement activity.	Data Security Implementation and best practices Enhanced security
ETSI TS 102 165-1 - Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) [i.12]	This document defines a method primarily for use by ETSI standards developers in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system.	Data Security Implementation and best practices Enhanced security

5.2.1.2 TC Human Factors (HF)

The Human Factors Technical Committee is the technical body within ETSI responsible for Human Factors issues in all areas of Information and Communications Technology (ICT). It produces standards, guidelines and reports that set the criteria necessary to build optimum usability into the emerging Digital Networked Economy (DNE).

The HF committee co-operates with other groups within ETSI and outside to assist them in producing standards, or other deliverables, which are in accordance with good Human Factors practice. Within ETSI it has a special responsibility for "Design for All" addressing the needs of all users, including young children, seniors and disabled people.

Table 2: Mapping of ETSI TC HF output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
ETSI EG 203 499 - User-centred terminology for existing and upcoming ICT devices, services and applications [i.15]	This guide aims at further simplifying end-user access to ICT devices, services, and applications by providing recommended terms for basic and commonly used ICT-related objects and activities, notably those terms that end users are commonly exposed to. Recommended terms are provided in 28 languages: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Icelandic, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Rhaeto Romance, Romanian, Slovak, Slovenian, Spanish, and Swedish (as spoken in their respective European countries).	Inclusion and Accessibility User-friendly solutions
ETSI EN 301 549 - Accessibility requirements for ICT products and services [i.16]	This document specifies the functional accessibility requirements applicable to ICT products and services, together with a description of the test procedures and evaluation methodology for each accessibility requirement in a form that is suitable for use in public procurement within Europe. It is intended to be used with web-based technologies, non-web technologies and hybrids that use both. It covers both software and hardware as well as services. It is intended for use by both providers and procurers, but it is expected that it will also be of use to many others as well.	Inclusion and Accessibility User-friendly solutions
ETSI TR 103 349 - Functional needs of people with cognitive disabilities when using mobile ICT devices for an improved user experience in mobile ICT devices [i.17]	The document contains a classification and analysis of usage needs of persons with limited cognitive, language and learning abilities (generically and historically referred to as "cognitive impairments"). It describes their functional needs for an improved user experience when using mobile ICT devices and applications.	Inclusion and Accessibility User-friendly solutions
ETSI EG 203 350 - Guidelines for the design of mobile ICT devices and their related applications for people with cognitive disabilities [i.18]	The document contains design guidelines for mobile devices and applications that will enable persons with limited cognitive, language and learning abilities (including people with age-related cognitive impairments) to have an improved user experience when using mobile ICT devices and applications.	Inclusion and Accessibility User-friendly solutions

5.2.1.3 TC Electronic Signatures and Trust Infrastructures (ESI)

TC ESI is responsible for standardization within ETSI supporting current and upcoming technology for trust services relating to Electronic Signatures and other trust services such as registered electronic delivery, electronic seals, electronic attestation of attributes and electronic archival. This includes trust service data formats, Identification procedures and policy and audit requirements for trust infrastructures supporting such trust services. This is aimed at supporting regulatory requirements such as the eIDAS Regulation as well as general international and commercial requirements.

NOTE: Many of the standards developed by TC ESI can be labelled as foundational in the context of age-verification and at the time of writing do not explicitly address age-verification although the work on selective disclosure does include the ability to release age-related attestations.

A significant element of the activity in TC ESI with regards to the stakeholder requirement addresses the governance, and each of the policy and security requirements, for matters relating to an individual and how data is released. This includes selective disclosure mechanisms.

Table 3: Mapping of ETSI TC ESI output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
ETSI TS 119 461: Policy and security requirements for trust service components for identity proofing [i.53]	Addresses identity proofing for issuing of (Qualified) Electronic Attestation of Attributes and use of such attribute attestations in identity proofing processes	Access control, identity and governance (Implementation and Compliance)
ETSI TS 119 462: Wallet interfaces for trust services and signing [i.54]		Access control, identity and governance (Implementation and Compliance)
ETSI TS 119 471: Policy and Security requirements for Providers of Electronic Attestation of Attribute Services [i.55] (in development)	Specifies the policy and security requirements of attribute attestation trust service providers and the attribute attestation services they provide, including: • Policy and security requirements on attribute verification and generation of attestations by the trust service provider; • Policy and security requirements on attribute attestation status validation services; • Requirements for assessing the trustworthiness of the attribute attestation; and • Requirements on personal data processing.	Access control, identity and governance (Implementation and Compliance)

Title of the Standard	Description	Stakeholder Requirement See Annex A
ETSI TS 119 475: Relying party authorizations for access to EUDI Wallet (in development) [i.56]	• Specifies requirements for qualified certificates attributes for electronic seals and website authentication, and qualified attestations of to be used by Relying parties in order to meet needs of eIDAS2 and ARF. • Specifies additional TSP policy requirements for the management (including verification and revocation) of additional attributes as required by the above profiles. These policy requirements extend the requirements in ETSI EN 319 411-2 [i.57]. • Specifies specific requirements for EU use of the qualified certificates for electronic seals, website authentication and qualified electronic attestations of attributers, to meet the requirements of the eIDAS2 and ARF.	Access control, identity and governance (Implementation and Compliance)

5.2.2 CEN/CENELEC

CEN, the European Committee for Standardization, is an association whose membership is composed of the National Standardization Bodies of 34 European countries.

CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes.

CEN supports standardization activities in relation to a wide range of fields and sectors including air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CEN has an agreement for technical co-operation with the International Organization for Standardization (ISO). Through the involvement of experts in Technical Committees, European and national expertise is being developed and recognized globally. The Vienna Agreement, signed in 1991, was drawn up with the aim of preventing duplication of effort and reducing time when preparing standards. As a result, new standards projects are jointly planned between CEN and ISO. Wherever appropriate priority is given to cooperation with ISO provided that international standards meet European legislative and market requirements and that non-European global players also implement these standards.

CENELEC, the European Committee for Electrotechnical Standardization, is an association whose membership is composed of the National Electrotechnical Committees of 34 European countries.

The high level of convergence between the European and international standards is facilitated by the ongoing technical cooperation between CEN and ISO through the Vienna Agreement and CENELEC and IEC through the Frankfurt Agreement. The main objectives of these agreements are to provide:

- A framework for the optimal use of resources and expertise available for standardization work, preventing duplication of effort and reducing time when preparing standards.
- Mechanism for information exchange between international and European Standardization Organizations (ESOs) to increase the transparency of ongoing work at international and European levels.

Table 4: Mapping of CEN/CENELEC output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
CEN/CENELEC - CWA 18016:2023 - Age-appropriate digital services framework [i.32]	The document includes reference to definitions and use cases for age assurance (including age verification and age estimation) and derives from the 5 Rights Foundation's policy development on the UN Commission on the Rights of the Child - General Comment 25 regarding children's digital rights. (This CWA is based on IEEE Std 2089™-2021, IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children [i.19]).	Implementation and best practices Rights and safeguards Respect children's Rights Inclusion and Accessibility User-friendly solutions

5.2.3 ISO/IEC

5.2.3.1 ISO/IEC General Information

The International Organization for Standardization (ISO) is an independent, non-governmental, international standard development organization composed of representatives from the national standards organizations of member countries. The organization develops and publishes international standards for the end-user or commoners' market, like availability in technical and non-technical fields, including everything from manufactured products and technology to food safety, transport, IT, agriculture, and healthcare.

The International Electrotechnical Commission (IEC) is an organization for the preparation and publication of international standards for all electrical, electronic and related technologies. These are known collectively as "electrotechnology".

ISO/IEC is currently embarking on the development of a series of standards covering age assurance systems. These standards are intended to provide a global framework for the development of further standards in specific contexts. They can also be used to define key vocabulary (as has been used in the present document) and understand the five core characteristics of age assurance (see clause 4.2 of the present document).

Table 5: Mapping of ISO/IEC output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Standard for Age Assurance Systems ISO/IEC DIS 27566-1 - Part 1: Framework [i.33]	At Draft International Standard (DIS) and is a global framework level document. It explores a number of Age Assurance Methods, including age verification, age estimation and age inference.	Implementation and Compliance International Standards
Standard for Age Assurance Systems ISO/IEC PWI 27566-2 - Part 2: Technical approaches and guidelines for use [i.34]	It relates to technical approaches and guidelines for use. It is a 'How to' document and looks at how to deploy and consider the different characteristics and what they may need in practical terms. It considers different deployments and variables, e.g. online and offline transactions.	Implementation and Compliance International Standards
Standard for Age Assurance Systems ISO/IEC AWI 27566-3 - Part 3: Benchmarks for Benchmarking Analysis [i.35]	It considers how to measure, analyse and assess the Age Assurance System. There are currently calls for this document to focus on Product Quality rather than Benchmarking, but this is undecided as of yet.	Implementation and Compliance International Standards

5.2.3.2 ISO/IEC JTC 1/SC 27 & SC37

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

Table 6: Mapping of ISO JTC1/SC27 output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
TR 15443-1:2012 - Information technology — Security techniques — Security assurance framework Part 1: Introduction and concepts [i.39]	It defines terms and establishes an extensive and organized set of concepts and their relationships for understanding IT security assurance, thereby establishing a basis for shared understanding of the concepts and principles central to ISO/IEC TR 15443 across its user communities.	Privacy and Data Protection
TR 15443-2:2012 - Information technology — Security techniques — Security assurance framework Part 2: Analysis [i.40]	It builds on the concepts presented in ISO/IEC TR 15443-1 [i.39]. It provides a discussion of the attributes of security assurance conformity assessment methods that contribute towards making assurance claims and providing assurance evidence to fulfil meeting the assurance requirements for a deliverable.	Privacy and Data Protection Implementation and best practices

Title of the Standard	Description	Stakeholder Requirement See Annex A
ISO/IEC 29115:2013 - Information technology — Security techniques — Entity authentication assurance framework [i.41] (under review)	It provides a framework for managing entity authentication assurance in a given context. In particular, it: • specifies four levels of entity authentication assurance; • specifies criteria and guidelines for achieving each of the four Levels of entity Authentication (LoA) assurance; • provides guidance for mapping other authentication assurance schemes to the four LoAs; • provides guidance for exchanging the results of authentication that are based on the four LoAs; and • provides guidance concerning controls that should be used to mitigate authentication threats.	Privacy and Data Protection Implementation and best practices
ISO/IEC 29128-1:2023 - Information security, cybersecurity and privacy protection — Verification of cryptographic protocols Part 1: Framework [i.42]	This document establishes a framework for the verification of cryptographic protocol specifications according to academic and industry best practices.	Privacy and Data Protection Implementation and best practices
ISO/IEC 27551:2021 - Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication [i.43]	This document provides a framework and establishes requirements for Attribute-Based Unlinkable Entity Authentication (ABUEA).	Privacy and Data Protection Implementation and best practices

5.2.3.3 ISO/IEC JTC 1/SC 37

Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards including common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross-jurisdictional and societal aspects.

Table 7: Mapping of ISO JTC1/SC37 output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
ISO/IEC 30136:2018 - Information technology — Performance testing of biometric template protection schemes [i.44]	It supports evaluation of the accuracy, secrecy, and privacy of biometric template protection schemes. It establishes definitions, terminology, and metrics for stating the performance of such schemes. Particularly, this document establishes requirements for the measurement and reporting of: • theoretical and empirical accuracy of biometric template protection schemes; • theoretical and empirical probability of a successful attack on biometric template protection schemes (single or multiple); and • the information leaked about the original biometric when one or more biometric template protection schemes are compromised.	Privacy-preserving methods Implementation and best practices
ISO/IEC 24714:2023 Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance [i.45]	This document gives general guidance for the stages in the life cycle of a system's biometric and associated elements. This covers the following: • the capture and design of initial requirements; including legal frameworks; • development and deployment; • operations, including enrolment and subsequent usage; • interrelationships with other systems; • related data storage and security of data; • data updates and maintenance; • training and awareness; • system evaluation and audit; • controlled system expiration. The areas addressed are limited to the design and implementation of biometric technologies with respect to the following: • legal and societal constraints on the use of biometric data; • accessibility for the widest population; • health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information.	Privacy-preserving methods Implementation and best practices

Title of the Standard	Description	Stakeholder Requirement See Annex A
	This document is intended for planners, implementers and system operators of biometric applications.	
ISO/IEC TR 30110:2015 Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children [i.46]	It provides guidance for users of biometric recognition systems on specific requirements in relation to deployments when children are included as subjects in the biometric process.	Privacy-preserving methods Implementation and best practices

5.2.4 ITU

The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for many matters related to information and communication technologies. The ITU promotes the shared global use of the radio spectrum, facilitates international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world. It is also active in the areas of broadband Internet, optical communications (including optical fibre technologies), wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, amateur radio, and next-generation networks.

The ITU addresses child online safety through a globally coordinated approach, guided by key resolutions like Resolution 179, WTDC Resolution 67 and Council Resolution 1306. The Child Online Protection (COP) Global Program focuses on advocacy, research, country-specific programs and child participation. Since the Correspondence Group on COP was established in March 2024, with a goal to focus on identifying and analysing deficiencies in existing international standards, and now aims to identify the gaps in addressing emerging threats and associated harms, and to lay the groundwork for robust and adaptable standards which prioritize the holistic protection of children in the digital world.

Table 8: Mapping of ITU output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Digiworld - An example of how the ITU Guidelines on Child Online Protection can be delivered in practice [i.36]	In this case study, explored how the ITU Guidelines on Child Online Protection (COP Guidelines) for industry and policymakers, parents, educators and children can be delivered effectively through cross-sector partnerships, co-design with local audiences and a shared vision for supporting children and families to thrive in a connected world.	Rights and safeguards: • Respect Children's right • Redress Mechanisms

5.2.5 IEEE

IEEE is a technical professional organization. IEEE and its members activities include publications, conferences, technology standards, plus professional and educational activities.

Table 9: Mapping of IEEE output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
IEEE 2089-2021 - Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children [i.19]	A set of processes by which organizations seek to make their services age appropriate is established in this standard. It sets out processes through the life cycle of development, delivery and distribution, that will help organizations ask the right relevant questions of their services, identify risks and opportunities by which to make their services age appropriate and take steps to mitigate risk and embed beneficial systems that support increased age-appropriate engagement.	Rights and safeguards Respect children's Rights Implementation and Compliance Ethical guidelines and user rights User-friendly solutions
IEEE P2089.2 - Standard for Terms and Conditions for Children's Online Engagement [i.20]	The standard defines processes and practices to develop terms and conditions that helps protect the rights of children in digital spheres. The standard helps avoid nudging, manipulation, and data exploitation that violate the interests of children. Furthermore, the standard enables providing data agency and ownership to children. The standard consists of the following clauses: (i) Age-appropriate digital content. (ii) Data sharing clauses. (iii) Artificial Intelligence (AI) access and manipulation of data. (iv) Transparency for data exchange. (v) Addiction to online services and related harmful components that cause exploitation and manipulation of children.	Rights and safeguards Respect children's rights Redress mechanisms Access Control and Content Limitation Transparency and information provision Clear information User Control
IEEE 2089.1-2024 - Online Age Verification [i.21]	Framework for the design, specification, evaluation, and deployment of online age verification systems are established in this standard.	Privacy and data protection Data security Compliance and governance
IEEE 2089.3 - Online Parental Consent (draft in-progress) [i.58]	Framework for the design, specification, evaluation, and deployment of online age verification systems are established in this standard.	Parental Consent Mechanisms

5.3 Age Verification Framework / Architecture

5.3.1 euCONSENT ASBL

euCONSENT ASBL is a non-profit organization, based in Belgium, formed to continue the work of a European Commission funded pilot project, initiated by the European Parliament of the same name.

euCONSENT's original architecture emulated eIDAS 1.0, redirecting users who had previously completed an online age verification to the original provider of that check, which could then confirm the answer to an age-eligibility question to a competing provider serving a different digital service.

euCONSENT is currently building a new decentralized, encrypted, tokenized interoperable solution, AgeAware, which moves to a decentralized model, to align more closely with eIDAS 2.0, and to incorporate privacy-enhancing technologies and a degree of device-based operation. This aims to address the evolving requirement of some European data protection authorities, notably the French CNIL and the Spanish AEPD, while maintaining an open and competitive commercial market for the provision of age assurance services. (This contrasts with an approach where Member States or, potentially, the EU itself develops, deploys, maintains and supports age assurance tools as a government service e.g. Spain's Digital Wallet Beta).

Table 10: Mapping of euCONSENT output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
AgeAware Specification - WP1: Business Requirements [i.47]	This document sets out the technical specification for a digital ecosystem which will facilitate an open and competitive market for interoperable, device-based, double-blind privacy-preserving age assurance.	Privacy and data protection Access Control and Content Limitation Transparency and Information Provision Rights and safeguards Implementation and governance Compliance and governance Ethical guidelines and user rights EUDI wallet and audits

6 Overview of National solutions and standards for Age Verification

6.1 Introduction

In this clause solutions and standards from national standards development organizations and official bodies will be identified and mapped to the relevant stakeholder requirement from clause 7 of ETSI TR 104 077-1 [i.7]. Also, copied and found in Annex A.

6.2 National

6.2.1 France

6.2.1.1 Association Française de Normalisation (AFNOR, English: French Standardization Association)

AFNOR acts as a central oversight body for standardization in France, identifies standardization needs and mobilizes interested parties. Strategic Committees (COS) organized by market or subject area are responsible for collective management of standardization programmes. Each COS brings together the main decision-makers in the economic sector concerned, defines work priorities and prepares French positions at international level with AFNOR representing France at CEN-CENELEC and ISO-IEC. Everything is coordinated by the Standardization Coordination and Steering Committee (CCPN) responsible for preparing the French standardization strategy, defining the objectives and general priorities of standardization programmes and ensuring their coherence relative to national, European and international policies.

Table 11: Mapping of AFNOR output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as CEN-CENELEC & ISO-IEC		

6.2.1.2 CNIL

Created by the French Data Protection Act of 6 January 1978, the Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority) is an independent administrative authority responsible for ensuring the protection of personal data contained in computer or paper files and processing operations, both public and private. On a daily basis, the CNIL ensures that information technology is at the service of the citizen and that it does not undermine human identity, human rights, privacy, individual or public liberties.

Table 12: Mapping of CNIL output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Demonstration of a privacy-preserving age verification process [i.22]	Is it possible to prove that one is over the age of legal majority without sharing one's age or identity? This demonstration is a possible implementation of an age-verification system that allows accessing restricted websites without sharing other personally identifiable data.	Privacy and Data Protection Access Control and Content Limitation Compliance and governance Implementation and governance Privacy by Design

6.2.2 Italy

6.2.2.1 Comitato Elettrotecnico Italiano (CEI, English: Italian Electrotechnical Committee)

It is responsible at a national level for technical standardization in the electrical, electronic and telecommunications fields, with direct participation - on behalf of the Italian State - in the corresponding European (CENELEC - Comité Européen de Normalisation Electrotechnique) and international (IEC - International Electrotechnical Commission) standardization organizations.

Table 13: Mapping of Comitato Elettrotecnico Italiano output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as CENELEC & IEC		

6.2.2.2 Ente Nazionale Italiano di Unificazione (UNI, English: Italian National Unification)

Performs regulatory activities in Italy across industrial, commercial, and service sectors, with the exception of electrical engineering and electronic competence of CEI. The UNI is recognized by the Italian State and by the European Union and represents Italian legislative activity at the International Standards Organization (ISO) and the European Committee for Standardization (CEN).

Table 14: Mapping of Ente Nazionale Italiano di Unificazione output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as ISO & CEN		

6.2.2.3 Agcom

The Communications Regulatory Authority (Agcom) is a "convergent" Authority. As such, it carries out regulatory and supervisory functions in the sectors of electronic communications, audiovisual, publishing, postal services and, more recently, online platforms. The profound changes brought about by the digitalization of the signal, which has standardized the transmission systems of audio (including voice), video (including television) and data (including Internet access), are the basis for the choice of the convergent model, adopted by the Italian legislator and shared by other sector Authorities at European and international level.

Table 15: Mapping of Agcom output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Linee guida parental control (Delibera n. 9/23/CONS) - Parental Control Guidelines [i.23]	Implementation of parental control measures by Website operators and examples of SCP activation and block operation.	Parental Consent Mechanisms

6.2.3 Ireland

6.2.3.1 National Standards Authority of Ireland (NSAI)

NSAI is responsible for the development of Irish Standards, representing Irish interests in the work of the European and International standards bodies CEN and ISO and creates, maintains and promotes accredited certification of products, services and organizations for compliance with recognized standards, from business management systems to product approvals.

Table 16: Mapping of NSAI output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as CEN & ISO		

6.2.3.2 Coimisiún na Meán

Coimisiún na Meán is Ireland's agency for developing and regulating a thriving, diverse, creative, safe and trusted media landscape. This means having a mix of different voices, opinions and sources of news. This means protecting children and all citizens from harmful content.

Their responsibilities are to:

- Oversee the funding of and support the development of the wider media sector in Ireland.
- Oversee the regulation of broadcasting and video-on-demand services.
- Develop and enforce the Irish regulatory regime for online safety.

Table 17: Mapping of Coimisiún na Meán output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Online Safety Code [i.24]	The Code is divided into two parts: Part A and Part B. Part A of the Code sets out the legislative and regulatory context for the Code and provides for the general obligations of video-sharing platform service providers. This includes the measures that video-sharing platform service providers are to take, as appropriate, to protect the general public and children. Part B of the Code makes provision for more specific obligations of video-sharing platform service providers and sets out the appropriate measures that video-sharing platform service providers are to take to provide the protections for children and the general public.	Implementation and Compliance Rights and safeguards Compliance and governance Implementation and governance Implementation and best practises Ethical guidelines and user rights

6.2.4 Spain

6.2.4.1 Asociación Española de Normalización y Certificación (AENOR, English: Spanish Association for Standardization and Certification)

AENOR is an entity dedicated to the development of Standardization and Certification in all Spanish industrial and service sectors.

Table 18: Mapping of AENOR output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as ISO & IEC		

6.2.4.2 AEPD

The Agencia Española de Protección de Datos (AEPD) / Spanish Data Protection Agency, the independent public authority responsible for ensuring the privacy and data protection of citizens. The objective of this space is, on the one hand, to encourage people to know their rights and the possibilities that the Agency offers them to exercise them and, on the other, to provide obliged subjects with an agile instrument that facilitates compliance with the regulations.

Table 19: Mapping of AEPD output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Decalogue of Principles - Age verification and protection of minors from inappropriate content [i.25]	The document lays out principles for the purpose of protecting minors on the Internet is to protect them from uncontrolled access to inappropriate content, which means that the ultimate goal is different from verifying their age or subjecting them to surveillance and monitoring. Inappropriate content for minors is freely accessible to those users who, having decided to access them, can prove that they meet the established age conditions.	Access Control and Content Limitation Rights and Safeguards Implementation and Compliance Parental consent mechanisms Privacy and data protection

Title of the Solution	Description	Stakeholder Requirement See Annex A
Cartera digital Beta app (Spanish age verification ecosystem) - Specification for the Use of the "Age of Majority" Credential [i.37]	This document outlines the specification for the Digital Wallet BETA project, which enables users to verify their age of majority to access adult content while maintaining anonymity. The system utilizes verifiable credentials linked to a Decentralized Identifier (DID) created from the user's public key. Each credential is issued in batches, allowing for multiple uses with the same content provider but preventing cross-provider tracking. The primary goal is to reduce user profiling and ensure anonymity during transactions.	Privacy and data protection**:** • Minimize data collection • Enhanced security • Data Deletion • Pseudonymization • Privacy Preserving Methods EUID Wallets and Audits Compliance and Governance Implementation and Governance
Cartera digital Beta app (Spanish age verification ecosystem) - Age Verification Protocol [i.38]	This technical specification document defines the communication protocol between user mobile applications and content providers for verifying age of majority. It outlines the necessary steps for requesting and presenting verifiable credentials to ensure interoperability at the national level. The document focuses on minimizing data disclosure and ensuring secure communication between stakeholders.	Privacy and Data protection Implementation and Best Practises

6.2.5 Germany

6.2.5.1 Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE, English: German Commission for Electrotechnical, Electronic & Information Technologies of DIN and VDE)

DKE constitutes a joint organization of DIN (the organization for general standards in Germany) and VDE (a technical-scientific association), the juridical responsibility for running the DKE being in the hands of the VDE. A standard may be first proposed by individual members of the VDE. Then when it has achieved national status, the standard then becomes sanctioned by DKE. If further the standard is adopted at an international level, it can become an IEC standard.

Table 20: Mapping of DKE output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
Same as IEC		

6.2.5.2 KJM

The Kommission für Jugendmedienschutz (KJM) is the central supervisory body for the protection of minors in private broadcasting and telemedia. Its remit is to ensure compliance with the provisions for the protection of minors that are enshrined in the Interstate Treaty on the Protection of Minors in the Media (JMStV).

Table 21: Mapping of KJM output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Criteria for evaluating concepts for age verification systems as elements for ensuring closed user groups in telemedia in accordance with § 4 para. 2 sentence 2 Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia (JMStV) [i.26]	Pursuant to the youth protection guidelines of the state media authorities, two interconnected steps are taken to ensure age verification for closed user groups: the first involves at least one-time identification (age of majority verification), which is carried out through personal contact. The second is authentication during the individual user process so as to effectively reduce the risk of access authorizations potentially being passed on to minors.	Access Control and Content Limitations Implementation and Compliance Compliance and Governance Implementation and governance

6.2.6 UK

6.2.6.1 British Standards Institution (BSI)

BSI produces British Standards, and, as the UK's National Standards Body, is also responsible for the UK publication, in English, of international and European standards. BSI is obliged to adopt and publish all European Standards as identical British Standards (prefixed BS EN) and to withdraw pre-existing British Standards that are in conflict. However, it has the option to adopt and publish international standards (prefixed BS ISO or BS IEC).

In response to commercial demands, BSI also produces commissioned standards products such as Publicly Available Specifications, (PASs), Private Standards and Business Information Publications. These products are commissioned by individual organizations and trade associations to meet their needs for standardized specifications, guidelines, codes of practice etc. Because they are not subject to the same consultation and consensus requirements as formal standards.

Table 22: Mapping of BSI output to stakeholder requirements

Title of the Standard	Description	Stakeholder Requirement See Annex A
PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice [i.50] (will be formally withdrawn when ISO/IEC 27566-1 [i.33] is adopted)	Some businesses have a legal requirement to conduct online age checks: whether because they sell age-restricted merchandise (e.g. dangerous goods); stream adult content; or provide age-sensitive services such as dating or gambling. This PAS helps these businesses comply with regulation, and safeguard their reputation, by providing recommendations that help prove an online user's age.	Implementation and Compliance Compliance and Governance

6.2.6.2 Childnet

Childnet is a UK-based charity for children, young people, and those who support them in their online lives, and its mission is to work with others to make the internet a safe place for children and young people.

Table 23: Mapping of Childnet output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Working with children and young people online [i.48]	As an organization reaches out to existing or new communities online, it is key that they have considered children's and young people's online safety as fundamental to their digital activity - whether their organization is youth facing or not. All online activities carry a level of risk, and this guide will help them understand and manage this.	Transparency and Information Provision: • Risk information • Digital literacy support

6.2.6.3 Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Table 24: Mapping of Childnet output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Age-appropriate design: a code of practice for online services [i.27]	The code is not a new law, but it sets standards and explains how the General Data Protection Regulation applies in the context of children using digital services. It follows a thorough consultation process that included speaking with parents, children, schools, children's campaign groups, developers, tech and gaming companies and online service providers.	Privacy and data protection Access Control and Content Limitation Rights and Safeguards Compliance and governance Implementation and governance Transparency and information provision
Age assurance for the Children's code [i.28]	The Children's code is a statutory code of practice. It sets out how Internet Society Services (ISS) likely to be accessed by children should protect children's information rights online. This opinion explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating the personal information risks children face online and facilitate conformance with the Children's code.	Transparency and information provision • User Control Implementation and Compliance • Compliance with legal standards Implementation and best practises

6.2.6.4 Ofcom

Ofcom is the regulator for the communications services that the UK uses and relies on each day. Also, Ofcom is the regulator for online safety in the UK, under the Online Safety Act. Their job is to make sure online services, like sites and apps, meet their duties to protect their users.

Table 25: Mapping of Ofcom output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services [i.29]	This guidance is for service providers that display or publish pornographic content on their online services to help them comply with their regulatory duties under the Online Safety Act 2023. These duties include a requirement for service providers to implement age assurance to ensure that children are not normally able to encounter pornographic content displayed or published on their service.	Compliance and governance • Legal compliance Implementation and best practises • Risk-based approach • Regular audits Transparency and information provision • User Control
Quick guide to children's access assessments [i.30]	Children's access assessments are a new assessment that all user-to user-services and search services ('Part 3 services') regulated under the Online Safety Act carry out to establish whether a service - or part of a service - is likely to be accessed by children. Services likely to be accessed by children will have additional duties to protect children online and they will need to also undertake a children's risk assessment and implement safety measures to protect children online.	Access Control and Content Limitation Compliance and governance • Legal compliance Implementation and best practises • Risk-based approach

6.2.6.5 National Cyber Security Centre (NCSC)

NCSC support the most critical organizations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, they provide effective incident response to minimize harm to the UK, help with recovery, and learn lessons for the future.

More specifically, the NCSC:

- understands cyber security and distils this knowledge into practical guidance that they make available to all;
- responds to cyber security incidents to reduce the harm they cause to organizations and the wider UK;
- uses industry and academic expertise to nurture the UK's cyber security capability;
- reduces risks to the UK by securing public and private sector networks.

Table 26: Mapping of NCSC output to stakeholder requirements

Title of the Solution	Description	Stakeholder Requirement See Annex A
Cyber Essentials [i.49]	It is a UK Government backed scheme that aims to help protect organizations, whatever its size, against a whole range of the most common cyber-attacks.	Privacy and data protection

7 Conclusions

This present document has identified that there are many available standards, solutions, frameworks and architectures to meet the stakeholder requirements for age verification. However, at this moment, there is not one currently deployed universal solution or standard which can meet all the stakeholders' requirements at an EU-wide level, though all the components to apply standards, solutions etc. for an age verification system are present. There are ones in development to be used at an EU-wide level.

At present, there is no fully developed, nationally focused system for age verification. Furthermore, implementing an EU-wide age verification system presents significant challenges. It would require design compromises that could undermine key objectives of age assurance, such as protecting user anonymity and ensuring that their online activities remain untraceable throughout the verification process.

The present document will be used as the starting point for ETSI TR 104 077-3 [i.59] which aims to define a set of proposals for the new work items to create standards for age verification.

Table 27: A summary of SDO activity mapped to the requirements from ETSI TR 104 077-1 [i.7]

Requirement (from ETSI TR 104 077-1 [i.7])	CEN	ETSI Cyber	ETSI ESI	ETSI HF	IEEE	ISO/IEC	ITU
Access control & content limitation			4		1		
Compliance and governance		6	4		1		
Data security		4					
Enhanced security		3					
Ethical guidelines and user rights					1		
EUDI wallets and audits							
Implementation and best practices	1	5				7	
Implementation and compliance		1	4		1		
Implementation and governance		5	4				
Inclusion and accessibility	1			4			
Parental consent mechanisms							
Privacy and data protection		8			1	5	
Privacy by design		2					
Privacy-preserving methods						3	
Redress mechanisms							
Rights and safeguards	1				2		
Support and education							
Transparency & information provision					1		
User-friendly solutions	1			4	1		

The highlighted rows show a gap from the SDOs. This is further explored in ETSI TR 104 077-3 [i.59].

Table 28: A summary of nation-state activity mapped to the requirements from ETSI TR 104 077-1 [i.7]

Requirement (from ETSI TR 104 077-1 [i.7])	France	Germany	Italy	Ireland	Spain	UK
Access control & content limitation	1	1			1	2
Compliance and governance	1	1		1	1	3
Data security						
Enhanced security						
Ethical guidelines and user rights				1		
EUDI wallets and audits				1	1	3
Implementation and best practices		1		1	1	
Implementation and compliance	1			1	1	1
Implementation and governance					1	
Inclusion and accessibility						1
Parental consent mechanisms			1		1	
Privacy and data protection	1				3	2
Privacy by design	1					
Privacy-preserving methods					1	
Redress mechanisms						
Rights and safeguards				1	1	1
Support and education						
Transparency & information provision						2
User-friendly solutions						

The highlighted rows show a gap from the listed nation-states which the SDOs may be able to provide standards for. This is further explored in ETSI TR 104 077-3 [i.59].

Annex A: Overview of Stakeholder Requirements from ETSI TR 104 077-1

Underage users of internet services and recipients of information groups requirements this annex outlines key requirements for underage users of internet services and recipients of information groups, based on guidelines and principles from documents identified in clause 6 of ETSI TR 104 077-1 [i.7]. The aim is to provide a holistic approach to age verification and the protection of minors online, ensuring that their digital interactions are both safe and enriching.

The following requirements have been identified:

Underage users of internet services and recipients of information groups requirements

a) Privacy and data protection:

- Minimize data collection: Age verification processes should collect only the minimum necessary data from underage users to achieve the intended purpose, thereby reducing the risk of data misuse.
- Transparency: It is essential to provide clear and accessible information to underage users about how age verification works, what data is collected, how it is used, and the measures in place to protect their privacy. This transparency helps build trust and ensures that young users are aware of how their information is handled.
- Enhanced security: Implementing enhanced security measures specifically tailored to protect the data of underage users is crucial. This includes secure data storage, encrypted communication channels, and regular security audits.
- Data deletion: Ensure that personal data is deleted immediately after verification to prevent unauthorized access and use of the data.
- Pseudonymization: Use pseudonymization techniques, such as data masking and hashing, to protect personal data, ensuring that it cannot be directly attributed to an individual without additional information (PAS 1296:2018 [i.50]).

b) Access Control and Content Limitation:

- Prevent access to harmful content: Mechanisms should be in place to prevent underage users from accessing content that is harmful or inappropriate. This includes using effective age verification systems and content filters.
- Parental control features: Providing robust parental control features allows parents to limit access to certain content or set time limits for use, thereby helping to create a safer online environment for their children.

c) Transparency and Information Provision:

- Risk information: Clear, age-appropriate information about the risks associated with internet use should be provided to underage users. This helps them understand potential dangers and how to navigate the digital world safely.
- Digital literacy support: Supporting the development of digital literacy skills in children is essential. Educational programs and resources should be made available to help them understand how to use technology responsibly and safely.

d) Rights and safeguards:

- Respect Children's Rights: Ensuring that children's rights are respected and protected in digital environments is a fundamental requirement. This includes their right to privacy, freedom of expression, and protection from exploitation.
- Redress Mechanisms: Providing clear channels for children to seek redress or challenge decisions related to age verification is important for maintaining trust and ensuring fair treatment.

e) Inclusion and Accessibility:

- Accessible Systems: Age assurance systems should be designed to be inclusive and accessible to all underage users, regardless of their socioeconomic status, race, or other characteristics. This ensures that no child is left unprotected due to systemic barriers.
- Avoid Discrimination: Age assurance systems should prevent discrimination against marginalized groups of children, ensuring equal protection and access to digital services for all.

f) Implementation and Compliance:

- Compliance with Legal Standards: It is critical to ensure that age verification systems comply with GDPR and other relevant regulations. This compliance helps protect user data and maintain the integrity of the verification process.
- International Standards: Adhering to international standards, such as IEEE 2089.1 [i.21] and ISO/IEC 27566 series ([i.33], [i.34] and [i.35]), ensures that age verification systems meet globally recognized benchmarks for quality and security (PAS 1296:2018 [i.50]).
- Privacy by Design: Implementing privacy-by-design principles into age verification systems ensures that privacy considerations are integrated into the development and operation of these systems from the outset.

Parents of underage users requirements

This subsection details the requirements for parents of underage users of internet services, highlighting how age verification systems and privacy measures can support them. The following requirements have been identified:

a) Parental consent mechanisms:

- Robust consent verification: Develop and implement secure systems to obtain and verify parental consent for underage users. This includes using multi-factor authentication or secure verification methods like government-issued ID checks.
- Specific consent: Ensure that parental consent is specific to particular data processing activities, allowing parents to make informed decisions about their children's data.

b) Transparency and information provision:

- Clear information: Provide clear, age-appropriate privacy information to parents about how age verification works, what data is collected, how it is used, and the measures in place to protect their children's privacy.
- Regular reporting: Maintain transparency by periodically reporting on age assurance practices to parents and other stakeholders.

c) Privacy and Data Protection:

- Privacy-preserving methods: Encourage the use of privacy-preserving age verification methods that do not require personal identification documents from parents. These methods should minimize data collection and adhere to privacy by design principles.
- Data minimization: Design parental consent mechanisms with privacy in mind, ensuring that only necessary data is collected and processed.

d) Support and education:

- Educational resources: Provide parents with resources about the importance of age verification and how to manage their children's online presence effectively.
- User-friendly tools: Develop user-friendly age assurance tools that are accessible and easily understandable for parents.

e) Rights and safeguards:

- Redress mechanisms: Create mechanisms for parents to easily revoke or manage their consent at any time, with changes taking effect promptly across all relevant online services.
- Parental control tools: Incorporate systems that include user-controlled mechanisms such as parental control tools to manage and restrict access to inappropriate content for minors.

f) Compliance and governance:

- Legal Compliance: Ensure that age verification systems comply with GDPR and other relevant legal frameworks, providing parents with confidence in the online services their children use.
- International standards: Adhere to international standards such as IEEE 2089.1 [i.21] and ISO/IEC 27566 series ([i.33], [i.34] and [i.35]) to ensure rigorous testing and certification of age verification systems.

Adult users of internet services and recipients of information groups requirements

This subsection details the requirements for adult users of internet services, emphasizing the importance of robust privacy measures, clear information provision, and secure data handling. The following requirements have been identified:

a) Privacy and data protection:

- Explicit consent: Obtain explicit consent from users before collecting any personal data. Ensure data minimization by collecting only the necessary information for age verification and other purposes.
- Privacy-preserving methods: Utilize advanced cryptographic methods, such as group signatures and zero-knowledge proofs, to allow users to prove their age without revealing any other personal information.
- Data security: Implement robust security measures to protect user data from unauthorized access and breaches. Ensure that all data collected is stored securely and used solely for the intended purposes.

b) Transparency and Information provision:

- Clear information: Provide transparent information to users about how age assurance tools are used, what data is collected, and the measures in place to protect their privacy. This includes details on data sources and how age verification is conducted.
- User control: Ensure that users have control over their data exchanges and the ability to manage their age verification tokens securely on their devices. Provide mechanisms for users to revoke consent and delete their data as needed.

c) Inclusion and accessibility:

- Accessible systems: Design age assurance systems to be inclusive and accessible to all adult users, including those without access to government IDs or advanced technology. Ensure that these systems do not discriminate against marginalized groups.
- Non-intrusive verification: Develop solutions that effectively verify age without being overly invasive, ensuring that privacy and convenience are balanced.

d) Rights and safeguards:

- Redress mechanisms: Provide clear channels for users to seek redress or challenge decisions related to age verification. Ensure that these mechanisms are easily accessible and user-friendly.
- Compliance with legal standards: Ensure compliance with GDPR and other relevant legal frameworks to protect user data and maintain the integrity of age verification processes.

e) Implementation and governance:

- International standards: Adhere to international standards such as IEEE 2089.1 [i.21] and ISO/IEC 27566 series ([i.33], [i.34] and [i.35]) to ensure rigorous testing and certification of age verification systems. Ensure continuous improvement and auditing of these systems to maintain their effectiveness and security (PAS 1296:2018 [i.50]).

- Privacy by design: Integrate privacy-by-design principles into all age assurance solutions, ensuring that privacy considerations are a core part of the system development and implementation process.

Providers of age verification services and national authorities providing age verification solutions

As digital services continue to expand, the need for reliable age verification systems becomes increasingly important. Providers of age verification services and national authorities ensure that these systems are not only effective but also respect user privacy and comply with legal requirements. This subsection details the essential requirements for these stakeholders.

a) Privacy and Data Protection:

- Data minimization: Collect only the necessary data required for verifying age and ensure that this data is stored securely and used solely for the purpose of age verification.

- Privacy-preserving methods: Utilize advanced cryptographic methods, such as group signatures and zero-knowledge proofs, to verify age without revealing other personal information (Demonstration of a privacy-preserving age verification process [i.22] (CNIL)).

- Data security: Implement robust security measures to protect personal data from unauthorized access and breaches. This includes encryption and regular security audits.

b) Transparency and information provision:

- Clear information: Provide transparent and accessible information to users about how age verification works, what data is collected, and the measures in place to protect their privacy (Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services [i.29] (Ofcom)).

- User control: Ensure that users can manage their data, including the ability to revoke consent and delete their information as needed (Age assurance for the Children's code [i.28] (Information Commissioner Office, ICO)).

c) Compliance and governance:

- Legal Compliance: Ensure that age verification systems comply with GDPR and other relevant regulations, such as the European Digital Identity Wallet (EUDI Wallet) Regulation (Decalogue of principles: Age verification and protection of minors [i.25] (AEPD, Spain)).

- International Standards: Adhere to international standards such as IEEE 2089.1 [i.21] and ISO/IEC 27566 series ([i.33], [i.34] and [i.35]), ensuring rigorous testing and certification of age verification system (IEEE Standard for Online Age Verification" (IEEE)).

d) Implementation and best practices:

- Risk-based approach: Develop risk-based assurance approaches tailored to different levels of online risk exposure.

- Regular audits: Conduct regular audits and reviews of age verification systems to ensure ongoing compliance and effectiveness.

e) Ethical guidelines and user rights:

- Ethical standards: Implement stringent ethical guidelines to protect user privacy and rights during the age verification process.

- User-friendly solutions: Design age verification solutions that are accessible and user-friendly, considering diverse user demographics, including children, adults, and individuals with disabilities (IEEE Standard for an Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children [i.19] (IEEE)).

Service/products providers subject to age verification obligations

This subsection details the essential requirements for service providers who need to obtain age information, emphasizing the importance of privacy, data protection, and compliance with legal standards.

a) Privacy and data protection:

- Data minimization: Ensure that the age verification process collects only the minimum necessary data from users, strictly limiting this to what is essential for verifying age.

- Preserving methods: Implement a privacy-preserving system where a third-party verifier conducts the age verification process without revealing the user's identity or the identity of the website requesting the information (Demonstration of a privacy-preserving age verification process" [i.22] (CNIL)).

- Data security: Implement robust security measures to protect personal data from unauthorized access and breaches. This includes encryption and regular security audits.

b) Transparency and information provision:

- Clear information: Provide transparent and accessible information to users about how age verification works, what data is collected, and the measures in place to protect their privacy ("Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services" [i.29] (Ofcom)).

- Parental consent: Obtain parental consent for minors to access certain content or services, ensuring that this consent is specific and informed.

c) Compliance and governance:

- Legal compliance: Ensure that age verification systems comply with GDPR and other relevant regulations, such as the European Digital Identity Wallet (EUDI Wallet) Regulation (Decalogue of principles: Age verification and protection of minors [i.25] (AEPD, Spain)).

- International standards: Adhere to international standards such as IEEE 2089.1 [i.21] and ISO/IEC 27566 series ([i.33], [i.34] and [i.35]), ensuring rigorous testing and certification of age verification systems (IEEE Standard for Online Age Verification).

d) EUDI wallet and audits:

- EUDI wallet: Comply with technical specifications for age verification mechanisms.

- Regular audits: Conduct regular audits and reviews of age verification systems to ensure ongoing compliance and effectiveness.

e) Ethical guidelines and user rights:

- Ethical standards: Implement stringent ethical guidelines to protect user privacy and rights during the age verification process.

- User-friendly solutions: Design age verification solutions that are accessible and user-friendly, considering diverse user demographics, including children, adults, and individuals with disabilities. (IEEE Standard for an Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children [i.19]).

Annex B:
The evolution of age verification and estimation with the adoption of AI techniques

Age estimation based on the mapping of human characteristics to age may use AI or Machine Learning processes to reach an estimation. Any use of AI is considered as High Risk under the AI Act and has therefore to have certain safeguards. The work of ETSI's SAI group and corresponding work in CEN/CENELEC JTC21 is therefore of relevance. A summary of the ETSI SAI activity and its relevance for age estimation using AI and ML techniques is given below.

Table B.1: Subset of ETSI TC SAI publications of relevance to age-verification and estimation

Reference	Title	Role in Age-verification and estimation
ETSI TR 104 031 (V1.1.1) (2024-01) [i.60]	Securing Artificial Intelligence (SAI); Collaborative Artificial Intelligence	Outlines the means to share models between systems. An AI system usually contains one or multiple AI Agents (AIAs), which learn and/or exploit an AI model based on different AI schemes such as deep learning, federated learning, reinforcement learning, and/or a combination of them. The report identifies risks and mitigations from developing collaboration between models and datasets across the AI lifecycle. In age estimation there may be a scope for models used in different environments to be shared with a view to increasing the efficacy of models, by extension of models (e.g. adding gait analysis to facial analysis).
ETSI TR 104 032 (V1.1.1) (2024-02) [i.61]	Securing Artificial Intelligence (SAI); Traceability of AI Models	
ETSI TR 104 225 (V1.1.1) (2024-04) [i.62]	Securing Artificial Intelligence TC (SAI); Privacy aspects of AI/ML systems	
DTR/SAI-007 (ETSI TR 104 048) [i.63] Expected publication Q1-25	Securing Artificial Intelligence; Data Supply Chain Report	
DTR/SAI-008 (ETSI TR 104 221) [i.64] Expected publication Q1-25	Securing Artificial Intelligence; Problem statement	
ETSI TR 104 062 (V1.2.1) (2024-07) [i.65]	Securing Artificial Intelligence; Automated Manipulation of Multimedia Identity Representations	The technology described by this standard is that which underpins multimedia masquerade and may allow an age-inappropriate person to present themselves as age-appropriate. Recognizing the techniques used is key to countering this form of fraud.
DTS/SAI-0014 (ETSI TS 104 223) [i.66]	Securing Artificial Intelligence TC (SAI); Cyber Security Requirements for AI	
DTS/SAI-0016 (ETSI TS 104 224) [i.67]	Securing Artificial Intelligence TC (SAI); Explicability and transparency of AI processing	

History

Document history		
V1.1.1	December 2024	Publication