ETSI TR 104 077-3 V1.1.1 (2025-02)

TECHNICAL REPORT

Human Factors (HF); Age Verification Pre-Standardization Study Part 3: Proposed Standardization Roadmap

Reference

DTR/HF-00301569

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

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 3 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.

1 Scope

The present document elaborates a set of proposals for further definition of work items within the standardization community to address the requirements identified in ETSI TR 104 077-1 [i.1] against the gaps identified and summarized in ETSI TR 104 077-2 [i.2].

The present document is intended for the SDOs identified in the proposals for their further consideration.

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 104 077-1: "Human Factors (HF); Age Verification Pre-Standardization Study Part 1: Stakeholder Requirements".

[i.2] ETSI TR 104 077-2: "Human Factors (HF); Age Verification Pre-Standardization Study Part 2: Solutions and Standards Landscape".

[i.3] Rudyard Kipling: "The Elephant's child", in Just So Stories, 1902.

[i.4] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

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

[i.6] European Commission, Working party on the protection of individuals with regard to the processing of personal data: "Opinion 05/2014 on Anonymisation Techniques".

[i.7] ETSI Technical Committee Securing Artificial Intelligence (SAI) Work programme.

[i.8] CEN/CENELEC JTC21 Work programme.

NOTE: CEN/CENELEC JTC21 works alongside ISO SC42 and is expected to consider the adoption of their output.

[i.9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence act).

[i.10] 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.11] ETSI TS 102 165-2 (V4.2.1) (02-2007): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

NOTE: An update is in development in ETSI TC CYBER planned for completion in late Q2-2025.

[i.12] ISO 7010:2019: "Graphical symbols — Safety colours and safety signs — Registered safety signs".

[i.13] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance).

[i.14] ETSI EN 301 549 (V3.2.1) (2021-03): "Accessibility requirements for ICT products and services".

[i.15] ISO 9241-210:2019: "Ergonomics of human-system interaction; Part 210: Human-centred design for interactive systems; Edition 2; 2019".

[i.16] Interaction Design Foundation: "Design for All".

[i.17] Centre for Excellence in Universal Design: "The 7 Principles".

[i.18] PubMed Central: "Exploring the Feasibility and Acceptability of Technological Interventions to Prevent Adolescents' Exposure to Online Pornography: Qualitative Research", JMIR Pediatrics and Parenting, 5 November 2024; 7:e58684. doi: 10.2196/58684.

[i.19] Yonder Consulting: "Adult Users' Attitudes to Age Verification on Adult Sites", 2022.

[i.20] IEA: "Why Online Age Verification will give us the worst of both worlds", 2024.

[i.21] EDRi (European Digital Rights): "Online age verification and children's rights", Position paper, 4 October 2023.

[i.22] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.23] Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act).

[i.24] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.25] 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.26] Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.27] Architecture Proposal for the German eIDAS Implementation.

NOTE: The proposal above includes an option to issue credentials in batches.

[i.28] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security Part 3: Vulnerability Assessment extension for TVRA".

[i.29] UNICEF: "The United Nations Convention on the Rights of the Child".

NOTE: A slightly modified children's version is available from https://www.unicef.org/child-rights-convention/convention-text-childrens-version.

[i.30] ETSI TR 103 936: "Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control".

[i.31] CNIL: "Online age verification: balancing privacy and the protection of minors".

[i.32] euCONSENT home webpage.

[i.33] euCONSENT: "AgeAware® Specification - Consultation Document".

[i.34] "Age verification system for access to online content: Age verification protocol".

[i.35] W3C® Group Note: "Verifiable Credentials Overview".

[i.36] Italian Legislative Decree 15 September 2023: "Urgent measures to combat youth hardship, educational poverty and juvenile crime, as well as for the safety of minors in the digital environment", (Caivano Decree).

[i.37] AGCOM Public Digital Identity System (SPID).

[i.38] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

[i.39] CEN/TC 224/WG 18 Work programme: "Interoperability of Biometric Recorded Data".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 104 077-1 [i.1], ETSI TR 104 077-2 [i.2] and the following apply:

estimation: determination of the value of a thing based on subjective criteria

NOTE 1: This is derived from the definition of age estimation given in ETSI TR 104 077-1 [i.1] and ETSI TR 104 077-2 [i.2] to distinguish from the term verification that relies on objective criteria.

NOTE 2: Estimation can itself use objective criteria in support of its determination.

high assurance level: assurance that ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with significant skills and resources

NOTE 1: A contextual definition is given in CSA Article 52.7 [i.23].

NOTE 2: A mapping from the CSA [i.23] definition to the metrics for risk analysis is given in ETSI TS 102 165-3 [i.28] and in ETSI TS 102 165-1 [i.22].

minor: someone who has not yet reached the age when they get full legal rights and responsibilities

NOTE: Taken from the law dictionary at https://www.legalchoices.org.uk/dictionary/minor.

substantial assurance level: assurance that the ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

NOTE 1: A contextual definition is given in CSA Article 52.6 [i.23].

NOTE 2: A mapping from the CSA [i.23] definition to the metrics for risk analysis is given in ETSI TS 102 165-3 [i.28] and ETSI TS 102 165-1 [i.22].

verification: confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 104 077-1 [i.1], ETSI TR 104 077-2 [i.2] and the following apply:

AI	Artificial Intelligence
AV	Age Verification
CAB	Conformity Assessment Bodies
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CNIL	Commission nationale de l'informatique et des libertés
CRA	Cyber Resilience Act
CSA	Cyber Security Act
DAC	Discretionary Access Control
EN	European Standard
ETSI	European Telecommunications Standards Institute
HF	Human Factors
IEEE	Institution of Electrical and Electronic Engineers
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MAC	Mandatory Access Control
SDO	Standards Development Organization
TC	Technical Committee
TR	Technical Report
TS	Technical Specification

4 Summary of identified standards gaps

From the analysis summarized in clause 7 of ETSI TR 104 077-2 [i.2], it can be shown that whilst standards exist across the SDO eco-system (see also ETSI TR 104 077-1 [i.1]) there are some gaps in the overall availability of standards. It is also clear from the analysis that there is a potential overlap of standardization activity that needs to be either eradicated, or clear guidance given to the applicability of each available standard to give assurance of age attestations. Table 1 is taken from clause 7 of [i.2] and has been copied and further annotated below using a traffic light system (summarized in the second column for accessibility purpose):

- Red (summarized by R and highlighted with corresponding row in darker colour) is used to indicate that there is no clear candidate standard available from an evaluated SDO;
- Amber (A) is used to indicate that multiple standards exist where clarification of their role in age verification is required; and
- Green (G) is used to indicate that a single standard exists that may be directly applied in age estimation subject to further analysis. The result from the applied colour coding is given in plain text after the table.

NOTE: The list of SDOs that have been analysed is necessarily truncated as a consequence of the resources available to prepare the present document and any follow-on activity recommended in the present document may identify additional resources that may be applied to age verification.

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

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

In summary, for each of the two topics of Ethics, and Transparency and Information Provision, only one SDO has been identified in the context of the study for the present document, given in ETSI TR 104 077-2 [i.2], namely IEEE for work on Ethics (see also clause 5.8 of the present document) and ETSI TC HF for matters relating to Transparency and Information Provision (see also clause 5.4 of the present document). No provisions from the SDOs that have been examined provide standards to address Support and Education, and similarly no SDO has been explicitly identified that addresses Parental Control, although for the latter many of the provisions for Access Control apply and this is addressed in more detail in clause 5.3 of the present document.

In similar manner to Table 1, a similar exercise filtering and classification of nation state activity has been summarized in ETSI TR 104 077-2 [i.2] and given in Table 2 below, using a similar traffic light indication of readiness as for Table 1, where green in this case indicates broad support of the topic, amber indicating only a single nation addressing the topic, and red indicating no support. The result from the applied colour coding is given in plain text after the table.

Table 2: A summary of nation state activity mapped to the requirements from ETSI TR 104 077-1 [i.1]

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

NOTE: The Digital Services Act [i.10], where applicable, may give pan-EU support to provisions of Rights and safeguards

In summary of the national provisions for age verification, none of the Member States that have been examined address the following topics for age verification: Data Security; Enhanced Security; Redress mechanisms; Support and Education; and User-friendly solutions. However, Table 2 has been composed with respect to standards and may be misleading as each of these topics is addressed by a mix of national law and by measures offered by more general standards and legislation.

5 Identification of proposed standards by requirement class

5.1 Overview

NOTE: The sub-headings in this clause are derived from the structure given in ETSI TR 104 077-1 [i.1].

Age verification can be viewed as a societal problem, a privacy problem and as a security problem. Standards in general, in the technical domain, do not seek to fix societal problems. It is considered naïve in the context of standardization for a complex societal issue such as age verification to expect a single standard, or even a suite of standards, to be able to tackle every eventuality. In particular, it is noted that there are a range of liabilities for violating age appropriate rules, laws and norms. It is also noted that some age appropriate restrictions require identification of the requesting party, whereas in many other instances age appropriate restrictions can be allowed to be wholly anonymous. In light of this, a solution for age verification that requires identification is not easily transposed to support a solution where anonymity is required or expected. Similarly, as social and national rules and conventions for age restrictions may differ across EU Member States (MS), and the material that such restrictions address is sufficiently diverse that it is considered unreasonable for the present document to recommend the development of a single solution supported by a single set of standards.

EXAMPLE: Classification of the age appropriateness of films has historically been treated differently in different regions. This is in part because of the local interpretation of the some or all of the following criteria:

1) **Cultural Sensitivities:** Different cultures have varying tolerance levels for violence, sexual content, and profanity.

2) **Legal Standards:** Each country has its own laws regarding media and censorship, influencing how films are rated.

3) **Historical Context:** Historical events and social movements can shape a country's perspective on certain content.

4) **Market Considerations:** Distributors may choose to appeal to broader audiences in certain countries, influencing how films are presented and rated.

The preceding reports (ETSI TR 104 077-1 [i.1] and ETSI TR 104 077-2 [i.2]) identify a large number of use cases, and those in turn identify a large number of regulatory constraints, and in some cases place legal liabilities on both the provider and accessor of age restricted services.

In light of the above, the present document does not recommend a single standard to address the topic of age assurance but does identify the areas where the requirements for age assurance have no corresponding standards and provide guidance and make recommendations on how to fill those gaps.

5.2 Privacy and data protection

The general security provisions that apply to both privacy protection, and data protection, are those of least privilege and least persistence. In both cases the role of data minimization is critical. A number of approaches to this exist, and many require the detailed process of a privacy and data impact assessment exercise. This essentially requires that the technical design, and policy design, of a system determines the answer to a number of questions prior to, and in the execution of, a system.

NOTE 1: The principle of least privilege is one that has a very long history predating the ICT domain and embraces a number of concepts. The first of these is that an asset is of value and that things of value should not be shared to those not needing to have it, this then as a second concept introduces the idea that it is possible to determine who has the right to access, and this then extends to identifying the things that can be done with an asset and applying restricted rights to each of them. As an example, in the ICT domain a privilege may be one of read, edit, delete, copy and a user may be granted one or more of these privileges. In summary least privilege access to a protected asset is to only allow those rights or privileges that are essential to perform the required task. In most access control systems that adopt least privilege the default is to deny (i.e. the least privilege is no privilege).

NOTE 2: Similarly to least privilege the concept of least persistence has a very long history that predates the ICT era. The concept of least persistence is that access to an asset is not granted forever, rather that access is granted for only sufficient time to perform the requested action. Least persistence is seen in most network systems where a resource is limited and shared (e.g. radio bandwidth, network capacity). Least persistence then ties into resource management as well as to security by taking steps to ensure that a resource is not hogged by any user.

Across ETSI a number of reports that address privacy have been published, in particular ETSI TR 103 370 [i.4], and the application of security controls defined in ETSI TR 103 305-5 [i.5] apply. As regards anonymity the Opinion 05/2014 on Anonymisation Techniques from the working party on the protection of individuals regarding the processing of personal data (article 29 group) [i.6] remains valid and underlines the technical difficulties of successful anonymisation as a tool of privacy. Further study into the role of Machine Learning and other Artificial Intelligence techniques on the provision of, or attacks on, anonymity and privacy in general are being pursued in ETSI TC SAI [i.7] and in CEN/CENELEC JTC21 [i.8] and are influenced by the EU Artificial Intelligence Act [i.9] and other global regulatory initiatives.

The following criteria should be applied to determine the role of data in a system (see Table 3). If no contextual answer can be given to any of the criteria it is reasonable to assert that the data should not be in the system.

NOTE 3: The criteria given below are named the Kipling criteria from their use in the short story "The Elephant's child", published in 1902 [i.3].

Table 3: Determination of role of data in a system considered for age verification

Kipling criteria	Example for data existence	Example for data access
What	What is the data?	What is the entity accessing the data?
Why	Why is that data in the system?	Why is that entity accessing the data?
When	When is the data meant to be available (e.g. is it ephemeral or persistent, if ephemeral how is it invoked and so forth)?	When is the data being accessed (is it being accessed at a reasonable time)?
How	How is the data used (e.g. what does it require in order to operate)?	How does the data know and verify that access is permitted?
Where	Where is the data (logically and geographically)?	Where is the entity with relation to the data (local or remote)?
Who	Who owns the data?	Who is the entity accessing the data?

There are a very large number of publications, including both standards and reports, from SDOs that address data privacy and data protection. The specific application of those standards to age verification is not defined and thus the citations given above cannot easily be applied. The relatively abstract nature of most such standards is often deliberate and where specific applications are considered they either exist in a vertical domain or as examples in a generic document.

5.3 Access control and content / functionality limitation

A general model for the provision of access control is given in clause 6 of ETSI TS 102 165-2 [i.11] addressing the technical means of achieving access control and the models of access control. In this there are two (2) primary models that are considered:

- Mandatory Access Control (MAC) - access to, and use of, the thing to which access is granted is wholly determined by the thing's owner.

- Discretionary Access Control (DAC) – the use of the thing to which access has been granted is at the discretion of the user and not addressed by the thing's owner.

EXAMPLE: For a MAC scheme the owner should be able to monitor the way in which the age restricted item to which access has been granted is used. This would make it difficult for an age appropriate user to access the item and then pass on its use to an underage user, whereas in a DAC model this is more feasible.

In addition, the means of asserting access are addressed by ETSI TS 102 165-2 [i.11] where the general model is attribute and policy based access control. In some cases, such as parental control, a third party is involved in addition to the owner of a protected resource. Whilst not strictly part of age verification, these are addressed here as they are identified in ETSI TR 104 077-1 [i.1] as a significant concern. Whilst this is not made explicit in ETSI TS 102 165-2 [i.11], the requirement to have parental consent can be modelled as an attribute of the access control scheme and further generalized as a requirement for 3rd party approval. What is more complex is making an external system aware of the relationship between the "parent" and the user.

RECOMMENDATION: Update ETSI TS 102 165-2 [i.11] to explicitly address the mechanisms for parental, or third party,control using age assurance as an example.

5.4 Transparency and information provision

Where age restriction is applied it should be made clear to all parties that age restriction applies. Where a violation of age restriction controls may lead to a penalty, it should be made clear what those penalties are and the jurisdiction that applies.

The liability may be placed on either, or both, the delivering or the consuming party and in all cases the liability of each party should be clearly identifiable at the point of delivery.

For age restricted content in the physical world, a large number of modes exist for signage and information but there does not appear to be a common standard. This lack of a common standard is extended into the ICT and online domain, where any such signage either copies the physical world format (e.g. for sale or supply of age restricted items such as tobacco products) or makes assumptions regarding data supplied by the subscriber (e.g. for media consumption).

It should be obvious to any user that age restriction is in force and affected users should be informed of the means by which age verification is carried out. In addition, where penalties exist for violation of age verification those penalties should be clearly identifiable.

NOTE: This is a devolved matter (i.e. each Member State of the EU can address this without requiring a common approach) and there may be no harmonisation of penalties.

A number of existing graphical symbols exist that may be modified to meet, at least in part, provisions for information provision (in the context of awareness). However, there is no universally accepted age verification symbol to be applied in either on-line or off-line systems.

5.5 Rights and safeguards

The United Nations convention on the rights of the child [i.29], in Article 17, protects the ability of children to access the opportunities provided by the Internet and by default has to be a consideration for any age assurance solutions deployed in a signatory jurisdiction. Consequently, for any age verification solution, safeguards have to be in place that balance the risk of harm with the benefits of access. Where access is in some way limited, the burden should be minimized on those who have a right to access.

NOTE: All UN member states except for the United States have ratified the Convention on the rights of the child [i.29].

The applicable text from [i.29] is quoted below:

QUOTE ([i.29]): *"Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand."*

The phrase "*… should make sure the information they are getting is not harmful*" is difficult in a standard's setting as harm is a moral and legal concept with many definitions. Standards which address objective criteria are often more straightforward to assess and determine conformance as opposed to those which address subjective criteria. In broad terms a guide or report can advise on the use of subjective criteria but cannot make mandates to follow that are allowed in technical standards that state objective criteria.

Legislation requiring age assurance has to be distinguished from legislation requiring identity verification. The technology deployed to prove age or age range should not inadvertently or deliberately disclose identity unless there is a specific legal requirement.

Similarly, an age assurance process should not become a vector of attack for monitoring the activities of a user online, unless there is a specific legal requirement for such surveillance.

Some forms of age assurance inevitably require the processing of personal data. The most obvious example would be the use of a conventional form of physical identification through which a user is authenticated and then the date of birth extracted as an age attribute. For as long as the age attribute is associated with a unique individual it would constitute personal data. A more complex case arises around the use of biometrics in age estimation solutions where an image for example may be the first input to the process, but it is then scanned and turned into a mathematical representation which is no longer uniquely identifiable to an individual. Depending on where this takes place in the technical architecture, it can mean that such a solution does not require a 3rd party to process any personal data because, for example the image has been turned into an anonymous representation at the device level. In terms of European data protection law, there is an argument that the data used for estimation purposes is not sensitive personal data because it can no longer be associated with a unique individual. However, this is a conclusion that has only been endorsed by the United Kingdom Information Commissioners Office and has not been confirmed by any European Union data protection authority, so the position within EU law remains unclear.

Where any age verification system makes use of personal data, this has to be in accordance with the prevailing data protection regime.

5.6 Inclusion and accessibility

No affected party can be excluded from participation in the age verification system. The provisions identified in clause 5.4 therefore have to ensure access to all.

Age verification systems/services therefore have to comply with the European accessibility act [i.13] that aims to improve the functioning of the internal market for accessible products and services by removing barriers created by divergent rules in Member States.

The products and services covered by the accessibility act include:

- computers and operating systems
- ATMs, ticketing and check-in machines
- smartphones
- TV equipment related to digital television services
- telephony services and related equipment
- access to audio-visual media services such as television broadcasts and related consumer equipment
- services related to air, bus, rail and waterborne passenger transport
- banking services
- e-books
- e-commerce

Where age verification is enabled for such services, it will be used through devices such as smartphones, computers, operating systems, and other online services. This means applying ETSI EN 301 549 [i.14], the scope of which addresses application to any type of ICT-based products and services. This includes software (web pages, mobile applications, desktop applications, etc.), hardware (smartphones, personal computers, information kiosks, etc.), and any combination of hardware and software.

Also applicable to age verification is ISO 9241-210:2019 [i.15], which provides requirements and recommendations for human-centred design principles and activities throughout the life cycle of computer-based interactive systems. It is intended to be used by those managing design processes and is concerned with ways in which both hardware and software components of interactive systems can enhance human-system interaction.

This means while no specific standard for accessibility in age verification will be needed, any standard or guidance for age verification should refer to existing accessibility standards such as ETSI EN 301 549 [i.14] and ISO 9241-210:2019 [i.15] when designing and developing the age verification tool, system or service.

It should also be noted that age verification may risk not meeting design for all [i.16] and universal design principles [i.17]. This includes the following design principles:

- Provide the same means of use for all users: identical whenever possible; equivalent when not.
- Avoid segregating or stigmatizing any users.

NOTE: By design age verification segregates users based on their age which should not be considered as a violation of the principle as the principle assumes that there is lawful right to the age restricted service.

- Provisions for privacy, security, and safety should be equally available to all users.
- Provide choice in methods of use.
- Eliminate unnecessary complexity.
- Provide compatibility with a variety of techniques or devices used by people with sensory limitations.

Design for all and universal design principles go beyond what is required from current accessibility legalisation. They are ideal recommendations but not a requirement.

RECOMMENDATION: TC HF and TC USER, and other SDOs they collaborate with, should ensure that provisions for Transparency and information provision are fully inclusive.

5.7 Implementation and compliance

The market for the provision of age verification services is diverse with a wide range of technologies, business models and technical architectures. The standards identified in the present document fall under a range of regulatory authorities, both statutory and non-statutory. So, implementation of these standards and the maintenance of compliance is complex.

There are some specialist Conformity Assessment Bodies (CABs) operating in the field of age verification, and there is the opportunity for these to operate across a range of disciplines – technical accuracy, data protection, accessibility, etc. Thus, these CABs can provide a holistic assessment of compliance with relevant standards when conducting age verification.

Regulatory authorities have to coordinate to ensure their requirements and enforcement activities are complementary. Some laws are interdependent. For example, a data protection requirement may only apply if particular content accessed by processing data is deemed harmful. The question of harm may be determined by another regulator not the data protection authority itself.

The field of age verification will benefit from co-regulation, where private sector actors are encouraged to seek third-party audit and certification against relevant standards, enabling them to signpost compliance authoritatively to regulators. In turn, regulators can then focus their scarce resources on organizations which do not exhibit conformity through certification.

Consideration should be given to a licensing regime where simply relying on compliance with law and regulation may not achieve sufficient public confidence in technologies. Given the potential to process substantial volumes of personal data, some of which may be considered special category data, even where this is avoided by applying privacy-by-design and data minimization principles, there may be an argument for providers of age verification services, or digital services which seek to implement age verification internally, to be subject to registration, dependent upon regular audit and certification.

5.8 Ethics

Ethics offers some difficulties in the domain of normative standards. The following characteristics (or tests) set out in ETSI's guide to developing standards should be embedded into the development of any contribution to a standard:

- **Necessary:** it (a standard) should specify only what is required to meet its objectives and not impose a particular approach to implementation.
- **Unambiguous:** it should be impossible to interpret the normative parts of the standard in more than one way.
- **Complete:** the requirement should contain all the information necessary to understand that requirement, either directly or by reference to other documents. The reader of a standard should not need to make assumptions about the implementation of any requirement.
- **Precise:** the requirement should be worded clearly and exactly, without unnecessary detail that might confuse the reader.
- **Well-structured:** the individual elements of the requirement should all be included in an appropriate and easy-to-read manner.
- **Consistent:** there should be no contradiction between different requirements within the standard, nor with other related standards.
- **Testable:** there should be clear and obvious means of demonstrating that an implementation complies with the requirement.

It is unlikely to be able to write technical requirements that provide mandates for the management of Ethics that satisfy all of the above criteria. However, that notwithstanding, it may be considered worthy to develop a guide to ethics specifically in the context of age verification.

RECOMMENDATION: Develop a report addressing the ethics of age verification from multiple stakeholder viewpoints. This may be derived in part from national and non-SDO work (e.g. euCONSENT [i.32]).

5.9 Accuracy

The designer of an age assurance system should define the expected accuracy of the system.

Where objective measures are used in determining a subject's age the allocation of attributes and verification data should be such that the likelihood of error should be close to zero (i.e. accuracy of the verification should be close to 100 %).

EXAMPLE: If the system asks for independent proof of the answer to the question "are you over 18?" the affected user should not be able to forge the proof.

Where subjective measures are used the measure of accuracy can be achieved by explicitly identifying the measure of precision and of recall against both static data and live data.

- Precision, the measure of positive predictive value, measures the correctness of the decision every time a positive decision is made. Precision can only be reliably measured against a known input (the number of relevant elements in any sample is known).

```
Precision = Number of true positives / (number of true positives + number of false positives)
```

- Recall is the measure of overall success at identifying relevant elements. As for precision, recall can only be reliably measured against a known input.

```
Recall = Number of true positives / (number of true positives + number of false negatives)
```

There are many other ways of measuring the system performance using other statistical measures, but the key point is that the system documentation should clearly indicate the measure by which the system claims to be accurate.

Metrics for accuracy of both subjective and objective claims should be standardized and cited by all age assurance systems. Where existing metrics exist it is strongly recommended to add an example of their application to age assurance.

6 Summary of recommendations

6.1 Overview

As stated in clause 5.1 age verification can be viewed as a security problem, a privacy problem and as a societal problem. Standards in general, in the technical domain, do not seek to fix societal problems. In addressing age assurance systems, those that are based on objective criteria can be tested relatively straightforwardly and should result in very high accuracy. By contrast any system based solely on subjective criteria are more difficult to apply testing to, and may result in either unacceptable levels of accuracy (see clause 5.9) or higher than acceptable levels of dispute.

The broad set of recommendations outlined in this clause extend and embellish the content of clause 5. In particular, it is suggested that future work concentrates on age verification where there is no physical presence of the asserting party (i.e. the party claiming age appropriateness is not physically present) and therefore considered mainly for online systems. It is recognized that across Europe there are a number of existing solutions proposed or implemented to address the problem (see Annex C), however the present document does not endorse any of these in particular but does suggest that the architectures, technologies and governance of each of those solutions (see Annex C for more detail) are taken into consideration in the development of future standardization.

In further addressing the scope of future work there should be consideration of motivation of users to break the age verification system (this is addressed in more detail in clause 6.3).

One item that needs more rapid attention is the terminology that surrounds age assurance. In this regard whilst some terms are offered in clause 3.1 there are many variations in how terms are used that alter their meaning. Effective standardization requires agreement on language and thus the terms used in the present document (and offered in clause 3.1) require further harmonisation to eliminate any uncertainty in their meanings.

6.2 Systems architectures

In common practice the architecture of a system should be clearly defined in order to ensure that a component can interface to the system with very high assurance of operability. As of the time of writing there is no such architecture and as a priority to enable further standardization this is essential.

The age assurance model and its architecture should be straightforward to understand and needs to be clearly written down in a form that solutions can refer to and show conformance to. The centre of the model is the age protected thing (shown in Figure 1 as "age restricted entity"), accessed by an age asserting party (shown in Figure 1 as "requesting entity") and held by a providing party (shown in Figure 1 as "liable entity"). For objective age verification the age asserting party holds the age assertion data, and the providing party has access to means that verify that data and the link to the age asserting party. The verification method itself will often involve one or more non-colluding parties and the decision to allow access is made by a policy maintained by the providing party, where the policy may be informed by the legal framework or jurisdiction in which the parties exist.

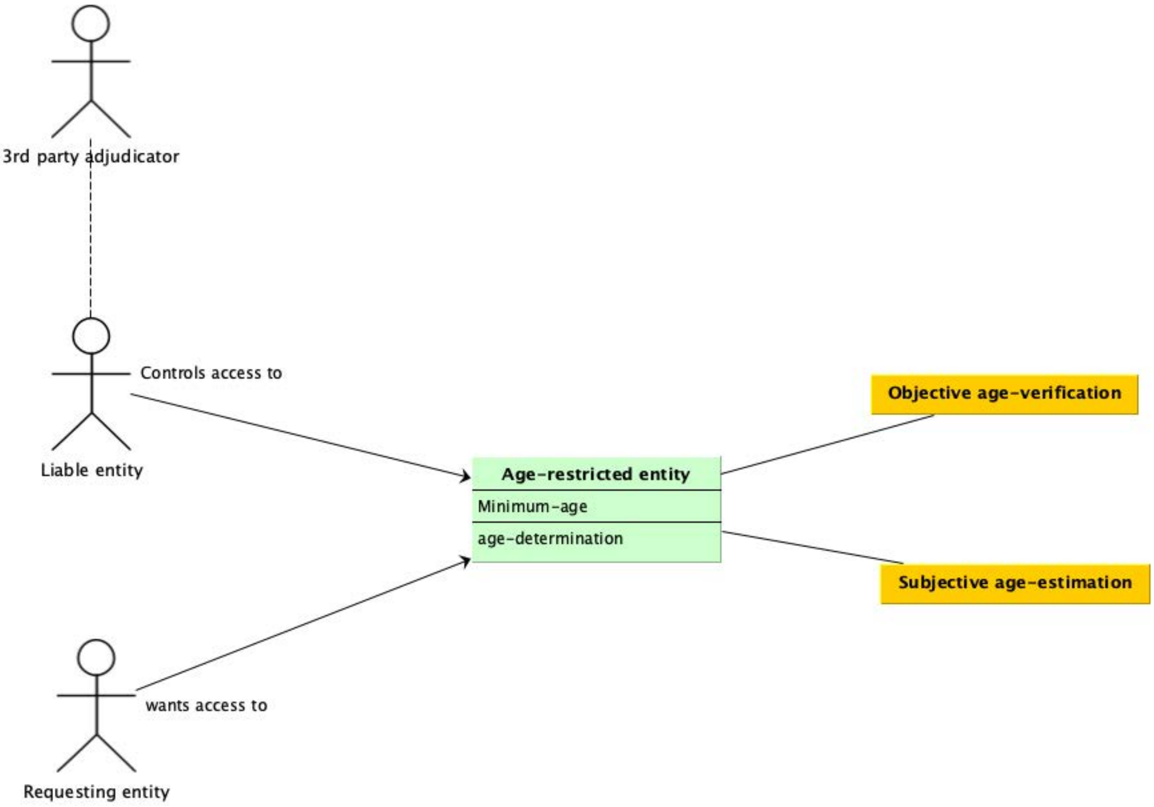

Figure 1: Simplified architecture of access to age restricted entity

The "age restricted entity" in Figure 1 is shown as having an attribute "Minimum age" and an associated method "age determination". The access control rule is relatively straightforward:

```
IF RequestingEntity.age IS GREATER THAN OR EQUAL TO MinimumAge
    PERMIT
ELSE
    DENY
```

There are many other architectural elements that can be added to this simple model to give assurance that the age attestation of the requesting entity is provably bound to the requesting entity, and to expand on the role of 3rd party adjudication (e.g. parental consent) in allowing the liable party to determine if access is allowed.

NOTE: The age determination method can be considered as a generalization of the "objective-age verification" and "subjective-age estimation" methods. In turn the "objective-age verification" may make use of other entities and architectures such as those in the Digital Wallet, and similarly "subjective age estimation" may make use of other entities and architectures including those for biometric age estimation.

6.3 Consideration of motivation

The role of motivation to break systems is addressed in Annex A of ETSI TS 102 165-1 [i.22] and in the metrics for determining risk in clause 6 of ETSI TS 102 165-1 [i.22]. For the purposes of the present document the role of attacker (as described in ETSI TS 102 165-1 [i.22]) is taken by the person attempting to access age inappropriate content, products or services and the system under attack is the entity able to offer age restricted content, products or services. For the present document the attacker may also be seen to act as an agent for other attackers, such as accessing age restricted content with the intent to sell it on to underage actors (see also discretionary access control in clause 5.3). Thus, the following key criteria may be considered when evaluating motivation and used to assist in the assessment of the practicality of countermeasures and the relative strength of the countermeasures:

- The likelihood of an attack:
    - If a threat is highly motivated an attack can be considered imminent, with a corollary of.
    - If a threat is unmotivated no attack can be anticipated.

- The value of the asset, monetarily or otherwise, to either the attacker or the asset holder:
    - An asset of very high value is likely to motivate an attack, with a corollary of.
    - An asset of little value is unlikely to motivate an attack.
- The expertise and resources with which an attacker is willing to effect an attack:
    - A highly motivated attacker is likely to acquire sufficient expertise and resources to defeat the measures protecting an asset, with a corollary of.
    - An attacker with significant expertise and resources is not willing to effect an attack using them if the attacker's motivation is low.

In each case there is no probabilistic means of determining the role of motivation in mounting an attack. However, in assessing threat potential it is essential to consider motivation in order to minimize the effect of motivation on the attacker. The metrics applied to motivation as defined in clause 6.6 of ETSI TS 102 165-1 [i.22] also apply with the following note.

NOTE: The wording in ETSI TS 102 165-1 [i.22] refers to threat agent as the agent of the person trying to bypass any age verification system. This is consistent with the use of the term system as the entity able to offer age restricted content, products or services and the measures they have put in place to protect themselves from releasing this to an age inappropriate user.

The motivation levels given in ETSI TS 102 165-1 [i.22] are as follows:

- Very low (indifferent)
- Low (curious)
- Medium (interested)
- High (committed)
- Very high (focused)

In age assurance systems, and particularly where social pressure is significant, there may be secondary or tertiary drivers to access age restricted content. For example there may be peer-pressure to access and share pornographic images, or alcohol, or to access an adult-oriented (but not pornographic) movie. The peer-pressure may be the dominant motivating factor and not the age restricted content. This form of motivating behaviour is often addressed as bullying or coercive control and has been given some consideration in ETSI TR 103 936 [i.30].

The motivation to access age restricted content is complex. Many of the studies cited (e.g. [i.18], [i.19], [i.20], [i.21]) identify some degree of harm from exposure to harmful content but mild forms of similar content are often seen as non-harming. However, studies have also identified weak content as a gateway or pathway to a desire to access stronger content. Motivation at an objective level is thus hard to address, but subjective motivation can be taken into account. Also, note that the broad examples given are only "correct" for a current country's cultural and social context. They change over time, for example the attitude towards, and portrayal of, smoking, from being something the vast majority partook in (and were encouraged to do so), to being discouraged and restricted.

EXAMPLE 1: Fashion magazines often show models in states of near undress, and partial nudity without exposure of certain erogenous zones is broadly acceptable in western European cultures, whilst full nudity through to sexual acts is frowned upon. The scale of acceptability is, as identified in clause 5.1, subject to many criteria and there is often no objective criteria for what should or should not be seen by minors. Michelangelo's David is both a stunning piece of art and also a very detailed representation of a nude man.

EXAMPLE 2: The sale of alcohol and the consumption of alcohol has similarly broad acceptability criteria although there are objective criteria for identifying a limit. This may mean restricting by the percentage of alcohol, the absolute volume of alcohol, or even the likelihood of alcohol. Thus natural fruit juices may, during storage, lightly ferment and over time have measurable alcohol content and could be made age restricted items even if at the point of placement on the market there is no measurable alcohol content.

EXAMPLE 3: In film and television there are both age classifications and looser constraints, for television broadcast, on the time of transmission of certain types of content. Again as identified in clause 5.1 this is a complex domain and whilst some objective measures can be applied (number of harsh swear words used in a given time) they are open to subjective determination (what is a swear word).

In addressing risk, and here the role of motivation in determining the likelihood of breaking protections, the guidance requested by instruments including the Cyber Resilience Act [i.24] is to provide protection commensurate with the risk. As the protection requested for access to age restricted content or services is some form of access control there has to be some degree of proportionality.

Proportionality is a thus a common theme in regulations requiring age verification.

The objective level of harm, and the means to prevent that harm is at the core of age verification. However it is also reasonable to state that a youth of 17 years and 11 months will not suffer massive harm that would not be suffered 1 month later. However, on the provider side, the harm has a different calculation and a minor error, say giving a youth of 17 years and 11 months access to a thing only legally permitted to be given to an 18 year old, where the age is known by objective data, has no leeway. The motivations of the provider and requestor may be different and again there may be a conflict between subjective reasoning and objective verification.

6.4 Transparency and explicability

As has been stated in clause 5.4 there is no universally accepted age verification symbol to be applied in either on-line or off-line systems.

Whilst a number of existing graphical symbols exist that may be modified to meet, at least in part, provisions for information provision (in the context of awareness) it is recognized that there is no universally accepted age verification symbol to be applied in either on-line or off-line systems. The example given in Figure 2 illustrates one such common application that adapts the P001 General Prohibition Symbol from ISO 7010:2019 [i.12].

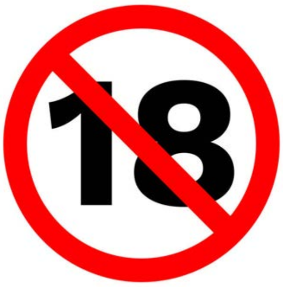

Figure 2: Common use of a prohibition symbol to represent age restrictions in force

6.5 Acceptability

For Age Verification (AV) technology, various research projects have found that generally people are in favour of AV but tend to express concerns regarding the specific implementation, data protection and privacy around it [i.18].

Though the majority of AV research focuses on intentional access of online pornography and there is broad support from adult users that have been surveyed for AV measures to prevent under-18s from accessing online pornography. AV measures are accepted where they are expected. For example, research participants said that they accept the requirement to verify their age whilst purchasing alcohol online or participating in online gambling. There is greater willingness to verify age to access online pornography if creating an account or subscribing to a creator to access content. Using a credit card is the preferred means of AV for paid access to pornography. Research participants express serious concerns about how user data may be processed and/or stored during AV processes to access pornography. This is reflective of a very low level of trust in the data privacy practices of adult sites. Privacy concerns could be addressed by increased transparency about how user data would be used, stored, and deleted; a choice of methods to verify age; and potentially independent third-party providers performing the age check, rather than the porn sites themselves [i.19].

It should be noted that in the USA where individual states mandated providers of adult content to implement age verification mechanisms on their websites often led some providers pulling access instead of implementing the AV measures and led to a rise in use of VPNs to access those sites instead [i.20]. But there is research which has identified AV measures which would be acceptable to users [i.21]. To be acceptable to the user, an age verification system would need to:

- Permanently prevent any linking of the internet activity or history to the person's identity, or to anonymous or pseudonymous profiles, ensuring that a person cannot be traced (i.e. 'zero knowledge').
- **Not provide any information to the provider other than a yes/no, and not facilitate any access by the provider or by a parent, guardian or other actor.**
- Ensure that anonymous use of the internet in general can continue.
- **Use tokens instead of storing personal data, and delete personal data processed for the purpose of generating the token immediately afterwards.**
- **Not allow any data collected or processed to be used for any other purpose.**
- Not allow the processing of biometric or biometric-based data.
- Refrain from requiring or encouraging all (young) people to have a digital ID, ensuring that people retain a right to analogue.
- **Be robust and secure from a cybersecurity perspective.**
- Be consensual, and not overly burdensome for those who do not want or do not have the means to verify their identity in this way.
- Be used only where strictly necessary.
- Be mindful of a potential chilling effect, in particular ensuring that access to educational and health (including reproductive health) material is not subject to age verification, which could have a chilling effect on whether or not children feel comfortable accessing this information.

From the above points it is possible to provide standards that address acceptability in age assurance systems either by updating existing ones or creating new ones to fill in the standards gap for some of these points as highlighted in bold and summarized below. It should be noted while users may want these provisions, they are not all implementable they should be considered advisory.

- **Not provide any information to the provider other than a yes/no, and not facilitate any access by the provider or by a parent, guardian or other actor.**
  - The assumption in this case is that the provider is able to ask only closed questions to which the answer is either yes or no, e.g. "are you over 18?".
  - The acceptability criterion in this case assumes that there is inherent trust in the system which is not the case for most real world systems.
- **Use tokens instead of storing personal data, and delete personal data processed for the purpose of generating the token immediately afterwards.**
  - Of itself a token is an ephemeral representation of part of the permission transaction. The token issuer has to have confidence that the requestor is age appropriate thus at the point of issue of the token personal data is processed (the requestor will then become the token holder). In overall liability the token issuer has also to trust that this token is not transferable to another age inappropriate party. The token consumer has to be able to validate the token without additional data from the token holder.
  - A token in this context is broadly equivalent to anonymised tokens in the physical world where tokens are by default anonymous and are interpreted as meaning the holder of the token is allowed to access the token accessible goods or services.

- **Not allow any data collected or processed to be used for any other purpose.**
  - This is addressed by legislation in Europe, primarily in the form of the GDPR [i.25], and by the general security principles of least privilege and least persistence.
- **Be robust and secure from a cybersecurity perspective.**
  - Within the broad EU context, illustrated by the CRA [i.24], it is required that cybersecurity provisions are commensurate with the risk of exploit of the system. Strong cybersecurity mechanisms often require strong means of authenticating the parties and may in turn require personal data to be given to some actors in the system so there needs to be careful balance of security with anonymity at point of use.

6.6 Security analysis of any proposed system

Age verification and age assurance systems that limit access to an asset are, broadly, access control measures (see clause 5.3). Whilst a detailed analysis of each possible method is out of scope of the present document the following guidance is offered in support of future work.

- Systems have to be resistant to collusion between actors that aim to subvert the control mechanisms.

EXAMPLE: If a 3rd party attestation of age appropriateness is used the relying party needs assurance that the 3rd party is not under the control of the accessing party to offer a false or misleading attestation.

- Systems should be designed to minimize the collection of data relating to an individual.
- Systems should be designed to limit the visibility of the relationship between a service provider and service recipient.

NOTE: This means that an observer should not be able to determine what age restrictions have been applied and to which product or service the restriction has been applied to.

For the purpose of analysis, the guidance of the Cyber Security Act (CSA) [i.23] and the Cyber Resilience Act (CRA) [i.24] should be taken into account. In particular as age restriction is broadly aimed at protection of minors the levels of security assurance that should apply are at least Substantial (CSA Article 52.6) and more likely High (CSA Article 52.7).

7 Conclusions

The present document is the last part of a three-part Technical Report that has analysed the user requirements (in part 1, ETSI TR 104 077-1 [i.1]), identified the existing standardization landscape (in part 2, ETSI TR 104 077-2 [i.2]) and made some recommendations to the standardization community – and ETSI in particular (in part 3, ETSI TR 104 077-3, the present document).

ETSI TR 104 077-1 [i.1] documents an analysis of the requirements of a large number of stakeholders across multiple online sectors which has revealed a very diverse range of requirements, driven by multiple pieces of legislation and divergent regulations. It provides a comprehensive overview of stakeholder requirements for age verification, that are essential for developing a standardized approach to age verification and age estimation solutions which will help align efforts across various sectors and jurisdictions, ensuring the protection of minors online while maintaining compliance with legal and regulatory requirements, encouraging the development of interoperable systems that can be easily adopted by service providers and verified by national authorities, together with ensuring all age verification solutions comply with GDPR [i.25], eIDAS2 [i.26], and other relevant laws provides a legal framework for data protection and user privacy.

ETSI TR 104 077-2 [i.2] identified many available standards, solutions, frameworks and architectures to meet the stakeholder requirements for age verification. However, the analysis fell well short of identifying a comprehensive universal solution or suite of standards which could address all these requirements at an EU-wide level, though all the components to apply standards, solutions etc. for an age verification system are present or 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.

ETSI TR 104 077-3 (the present document), has been developed from the findings of the parts 1 and 2, and asserts that it is not feasible to outline a single technical solution. Consequently, the present document focuses on identifying the areas where the requirements for age assurance have no corresponding standards and provides guidance and makes recommendations for a work programme of the Standards Development community on to fill those gaps:

- Which kind of additional standards documents should be developed (with the possible addition of a recommended body for undertaking the associated work).
- Which kind of technical approach could be considered in the above developments. The key technology components to be considered are identified as acceptability, accessibility, security and privacy.

Once a full set of standards is in place, the market may produce one or more technical solutions that conform to those standards and emerge as the solution which itself becomes standardized.

Annex A: Template work item lead TB, scope statements and document formats for ETSI activity in support of age verification

A.1 TC CYBER

A number of points are identified in the preceding analysis where additional consideration should be given by TC CYBER to issues related to age assurance. In particular examples of the role of age assurance should be added to the considerations of risk analysis in the ETSI TS 102 165 series of specifications ([i.11], [i.22], [i.28]). Whilst this may be focussed on access control there are identified considerations for motivation and for testing to be addressed.

It is also noted in clause 6.3 and to a lesser extent in clause 6.6 that age verifications, and bypassing them, may be included as a consideration of coercive behaviour and this may be taken into account in ETSI TR 103 936 [i.30].

A.2 TC HF and TC USER

In close collaboration with associated groups in CEN/ISO it is recommended, from the analysis presented in clauses 5 and 6, and identified in the conclusions of clause 7, that TC HF and TC USER address the domains of transparency and information provision, particularly with regards to signage elements for both online and offline age assurance schemes.

It is suggested that the signage is developed as a Technical Specification format (this may be any of TS, ES, EN). A preference to develop an EN is suggested as this has potential for wider reference by the NSOs in national actions.

A.3 TC ESI

The extensions of eIDAS to address the digital wallet and the role of each of selective disclosure and of verifiable credentials is developed it would be useful to further address this in the ESI activity with explicit mention of the role in age verification.

Annex B: Template work item descriptions for activity in support of age verification in other SDOs

B.1 CEN/ISO

As noted in clause A.2 work on common signage is required and this should be carried out in harmonisation with work in ETSI. In addition, although not stressed strongly in the present document, the role of biometrics in age estimation that is considered in CEN (CEN/TC 224/WG 18 [i.39] - Interoperability of Biometric Recorded Data) should include age estimation in its examples and scope.

B.2 IETF, W3C and associated communities

Many of the recommendations across the present document (all parts) are applicable to technologies that are standardized by activities taking place in the global standardization community dealing with age verification. Whilst the primary recommendations are to ETSI and the ESOs it is recognized that any work undertaken in those may be taken into account in the work taking place in groups including IETF, W3C and their associated communities. The ESOs may be in a position to drive the work as well as refer to the outcome of other groups.

Annex C:
Existing solutions (partial, or otherwise)

C.1 Existing industry practice – third party age assurance with data minimization

In a jurisdiction where there is an effective data protection regime systems of age verification which rely on a 3rd party to confirm the age or age range of a user and then only to pass on to relying parties' confirmation of whether users meet a particular age requirement provide sufficient protection against privacy breaches.

NOTE: The existing GDPR [i.25] addresses data in general and by default addresses personal data including age. The GDPR does not however deal directly with age assurance but the mechanisms of consent that it does address are consistent with the requirements for age assurance.

C.2 France: CNIL/ARCOM "double-blind" prototype

The French Data Protection Authority has been an advocate for additional technical measures to further guarantee privacy which go beyond reliance on the rule of law and introduce privacy enhancing technologies to protect both the individual's identity and prevent any record of their online behaviour being created as a result of age verification. The relevant mechanisms are described in [i.31].

It should be noted that this approach still relies on compliance with the legal requirements in place and may not provide any additional insurance against misbehaviour by bad actors than existing industry practice. But the use of such technologies may serve to improve public trust in the age verification process.

C.3 Spain: Age Verification on-device application

The Spanish Data Protection Authority has been particularly concerned that an age verification process may enable bad actors to identify minors on the Internet. It advocates for solutions which operate age verification entirely locally on the user's device and minimize the opportunity for relying parties to become aware of whether a user is a child or not. An age verification app on a device confirms the user's age from a digital identity such as the European digital identity wallet and then confirms to the devices apps and any websites accessing through the device's browsers whether or not the user meets an age requirement. Critically it should be ambiguous whether a user failed to pass a test because they were a child or for some other reason.

The Spanish system [i.34] is based on verifiable credentials described by W3C and found in [i.35].

C.4 Italy: AGCOM Public Digital Identity System (SPID) "double anonymity" model

The Italian AGCOM's proposed "double anonymity" model for age verification, outlined in its draft regulation of 24 September 2024 [i.37], ensures robust privacy protections while fulfilling legal requirements to safeguard minors from harmful online content. The system, developed under the "Caivano Decree" [i.36] and aligned with EU legislation such as the Digital Services Act [i.10], incorporates principles of proportionality, data protection, and transparency.

The model divides the verification process into distinct phases to ensure separation of responsibilities and prevent data misuse. Certified independent third parties issue a "proof of age" after verifying the user's identity. These entities do not know the purpose of the verification, ensuring that users' intentions remain private. The proof is then securely communicated to the user, who presents it to the service provider. The provider determines access eligibility based solely on the proof, without further data exchange.

For application-based systems, proofs of age can be generated and managed directly via digital identity apps on user devices, leveraging the European digital identity framework. The model also mandates session-based age verification, ensuring continuous protection with minimal data retention.

AGCOM's framework emphasizes technological neutrality, allowing flexibility for providers while ensuring compliance with rigorous standards, including security, accessibility, and inclusivity. By obfuscating failure reasons, the system prevents profiling and discrimination against minors. This approach not only meets the requirements of Italian and European legislation but also establishes a scalable, privacy-first model for protecting minors online.

C.5 euCONSENT: AgeAware® tokenized ecosystem

euCONSENT [i.32] a non-profit organization based in Belgium created to take forward the work of a European Commission funded project of the same name has developed a specification for an interoperable tokenized solution which is claimed to deliver similar benefits to the French and Spanish approaches. When a user completes an age verification process with a third party provider they may agree to accept a token on their device which contains an age attribute this may be either the specific date of birth or an age range which has been confirmed to a particular level of assurance. When the user seeks to access another digital service either the service or its 3rd party age verification provider may read the token confirm the signature and then reuse a previously completed age check without further imposition on the user. This ecosystem also incorporates a tallying service to facilitate the commercial operation and enable age verification providers to charge a third party for the use of their age checks and an anonymisation service to prevent any token being subverted in a way which allows for the tracking of an individual's online behaviour.

The AgeAware® system is described in [i.33].

C.6 EUDI Wallet: batch issuance

The European Union has been working towards the delivery of a European digital identity wallet available to all citizens by the end of 2026. This may be a suitable mechanism for age verification through this selective disclosure of an age attribute. Though if some debate about whether this can be done in a way which meets the requirement for anonymity given the underlying architecture of the wallet. Recognizing these concerns, a workaround has been developed which enables the wallet to issue a batch of certificates with age attributes that can then be used in a way which obfuscates the unique identity of the user [i.27].

NOTE: There are broad similarities between the obfuscation technique of batch issuance and the pseudonymous attribute certificates used in the cooperative Intelligent Transport System defined in ETSI TS 102 940 [i.38].

Annex D (informative): Bibliography

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

History

Document history		
V1.1.1	February 2025	Publication