



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

### **Document Preview**

[ETSI TR 104 077-3 V1.1.1 \(2025-02\)](https://standards.iteh.ai/catalog/standards/etsi/8202c8fa-86aa-4418-931b-977dc6eb9612/etsi-tr-104-077-3-v1-1-1-2025-02)

<https://standards.iteh.ai/catalog/standards/etsi/8202c8fa-86aa-4418-931b-977dc6eb9612/etsi-tr-104-077-3-v1-1-1-2025-02>

---

**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**

---

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 2025.  
All rights reserved.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope .....	6
2 References .....	6
2.1 Normative references .....	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations .....	9
4 Summary of identified standards gaps .....	9
5 Identification of proposed standards by requirement class .....	11
5.1 Overview .....	11
5.2 Privacy and data protection .....	11
5.3 Access control and content / functionality limitation .....	12
5.4 Transparency and information provision.....	13
5.5 Rights and safeguards.....	13
5.6 Inclusion and accessibility.....	14
5.7 Implementation and compliance.....	15
5.8 Ethics .....	16
5.9 Accuracy.....	16
6 Summary of recommendations.....	17
6.1 Overview .....	17
6.2 Systems architectures .....	17
6.3 Consideration of motivation .....	18
6.4 Transparency and explicability.....	20
6.5 Acceptability .....	20
6.6 Security analysis of any proposed system .....	22
7 Conclusions .....	22
<b>Annex A: Template work item lead TB, scope statements and document formats for ETSI activity in support of age verification.....</b>	<b>24</b>
A.1 TC CYBER .....	24
A.2 TC HF and TC USER.....	24
A.3 TC ESI.....	24
<b>Annex B: Template work item descriptions for activity in support of age verification in other SDOs.....</b>	<b>25</b>
B.1 CEN/ISO .....	25
B.2 IETF, W3C and associated communities .....	25
<b>Annex C: Existing solutions (partial, or otherwise) .....</b>	<b>26</b>
C.1 Existing industry practice – third party age assurance with data minimization .....	26
C.2 France: CNIL/ARCOM "double-blind" prototype.....	26
C.3 Spain: Age Verification on-device application .....	26

C.4	Italy: AGCOM Public Digital Identity System (SPID) "double anonymity" model.....	26
C.5	euCONSENT: AgeAware® tokenized ecosystem .....	27
C.6	EUDI Wallet: batch issuance .....	27
<b>Annex D (informative):</b>	<b>Bibliography.....</b>	<b>28</b>
History .....		29

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

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

<https://standards.iteh.ai/catalog/standards/etsi/8202c8fa-86aa-4418-931b-977dc6eb9612/etsi-tr-104-077-3-v1-1-1-2025-02>

---

# 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