ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies"
Convenorship: **DIN**
Convenor: **Rannenberg Kai Mr Prof. Dr.**

ISO/IEC AWI 1st WD 27566 Age Assurance Systems

Document type	Related content	Document date	Expected action
Ballot / Reference document	Ballot: ISO/IEC AWI 27566 (restricted access)	2023-05-25	**COMMENT/REPLY** by 2023-08-31

ISO #####-#:####(X)

ISO/IEC JTC1/SC27/WG5

Secretariat: DIN

Information security, cybersecurity and privacy protection – Age assurance systems – Framework

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes d'assurance de l'âge - Cadre de travail

WD1.2

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

To help you, this guide on writing standards was produced by the ISO/TMB and is available at https://www.iso.org/iso/how-to-write-standards.pdf

A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC1 Information Technology, Subcommittee SC27, Information security, cybersecurity and privacy protection, Working Group WG5, Identity Management and Privacy Technologies.

This is a first edition.

A list of all parts in the ISO ##### series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This International Standard sets out a framework and core principles for age assurance systems deployed for the purpose of enabling age-related eligibility decisions by anybody for any reason in any location through any type of relationship between a natural person and the provider of any product, content or service that has policy requirements for acquiring assurance about the age of persons (such as the supply of alcohol, tobacco, weapons or online content).

Age-related eligibility decisions are based on the fact that a person should either be older or younger than a given threshold age or be within an age range, where ages are counted in years and where these criteria are dependent upon the type of goods, content or service to be provided.

This document aims to solve the problem of inadequately defined age assurance processes and associated lack of trust and recognised benchmark against which the systems can be scored in terms of efficacy, acceptability, privacy and security.

Although a natural person's age is an attribute of their identity, it is not necessarily the case that establishing the full identity of a natural person in a global context is needed to gain age assurance. As such, the process of age assurance may in some instances be connected to identity verification, but can also be performed in ways other than via identity verification.

The aim of this Standard is to enable policy makers (like government, regulators or age restricted product, content or service providers) to specify applicable types of age assurance systems and indicators of confidence in their particular policy requirements.

As an example, a policy maker may determine that, in order to authorise the sale of liquor, a decision maker 'shall use some specific type of age assurance systems and a set of indicators of confidence in accordance with ISO [Standard Reference]' or in order to authorise an actor to participate in filming for an adult production, a decision maker 'shall use other type of age assurance systems with a different set of indicators of confidence in accordance with ISO [Standard Reference]'. This standard does not determine which type of age assurance system nor which set of indicators of confidence are appropriate for each type of age-related eligibility decision – that is a matter for policy makers..

This Standard does not:

- Establish or hinder the establishment of any methodologies (called assurance components in this standard) for age assurance systems
- Establish or recommend the age assurance thresholds or determine the required indicators of confidence for different products, content or services – these are matters for policy makers
- Deal with financial or commercial models for age assurance systems – these are a matter for economic operators in the age assurance process
- Address, save for some specific objectives applicable to age assurance systems, the requirements for securing data protection and privacy of persons – these are a matter for data controllers
- Establish the detailed requirements for interoperability, age assurance trust frameworks, age assurance exchanges or communities of interest for age assurance systems – these could be a matter for future standards, technical specifications or technical reports

The International Organization for Standardization (ISO) *[and/or] International Electrotechnical Commission (IEC)* draw[s] attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO *[and/or] IEC* take[s] no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO *[and/or] IEC* that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO *[and/or] IEC*. Information may be obtained from the patent database available at www.iso.org/patents.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO *[and/or] IEC* shall not be held responsible for identifying any or all such patent rights.

Information security, cybersecurity and privacy protection – Age assurance systems – Framework

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes d'assurance de l'âge - Cadre de travail

1 Scope

Editor's Note: The scope as per the New Work Item Proposal and balloted on is:

This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about the age of, or an age range for, a natural person.

Editor's Note: The ISO/IEC JTC1 SC27 WG5 Experts reviewed the scope statement on 2023-04-18 and considered that it ought to be amended as shown. This will, in due course, require a further P-member ballot, but for now, that is held back pending any other expert comments on scope from the Call for Contributions.

Proposed Scope

This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about an age threshold of, or an age range for, a natural person.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*

ISO/IEC 30107-1:2016, *Information technology – Biometric presentation attack detection – Part 1:Framework*

... [There are more to include here]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

Editor's Note: The SC27/WG5 Experts consider that some of the definitions in this section are either unnecessary or may benefit from re-wording. In particular, definitions should be drafted to be replaceable

in the text in the body of the document and, in some cases, this would make them unwieldy. Views and suggestions are welcome in the call for contributions and comments on improvements to the definitions.

3.1
age assurance
process of establishing, determining, and/or confirming an age determination attribute

3.2
age assurance practice statement
document describing the operational practices and procedures of an organisation that provides assured age attributes or is responsible for making age eligibility decisions

3.3
age assurance provider
organization responsible for processes establishing or computing age attributes

3.4
age assurance service
service provided individually or collectively by age assurance providers

Note to entry: An age assurance service can consist of one or more organizations

3.7
age category criteria
quantitative formulation describing age conditions to be fulfilled to be in accordance with the law or with some regulations or with some commercial offers

3.8
age determination
indication that a natural person is over or under a certain age or within age range

3.10
age estimation
age determination performed using inherent features or behaviours related to a natural person

3.12
age-related eligibility
right of access to goods, content or services based on an age limit or an age band

3.13
age determination attribute
attribute indicating an age determination (3.8) associated with a natural person

3.14
age attribute broker
organization responsible for securing and disseminating a subject's age attributes, but that is not an age assurance provider

3.15
age verification
age determination based on the validity of a credential that provides information that directly allows calculating the difference computation between the current date and the date of birth of the natural person as presented in a valid credential

3.16
age inference
age determination based on the validity of a credential that provides information which indirectly allows to determine that a natural person is over or under a certain age

3.17
artificial intelligence
branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement

[SOURCE: ISO/IEC 2382:2015, Information technology — Vocabulary]

3.18
assurance component
component that captures, analyses, gains confidence in or disseminates age determination attributes of a natural person

3.19
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

Note to entry: attack vector can include IoT devices, smart phones etc.

[Source: ISO/IEC 27032:2012, 4]

3.20
attested PII
electronic attestation of PII that contains PII from a relevant authentic source issued by an authoritative body or by a designated intermediary recognised at an appropriate level

Editor's Note: The SC27/WG5 Experts debated whether this should refer to national level, appropriate level, resource server level or some other recogniser of an authentic source.

3.21
attribute
characteristic or property of an entity

[SOURCE: ISO/IEC 24760-1: 2019, 3.1.3]

Note to entry: within the context of this document, the entity is a natural person.

3.22
attribute aggregation
mechanism of aggregating attributes of a user originating from multiple sources

3.23
attribute server
server trusted by one or more natural persons and one or more resource providers to issue attributes related to a natural person

3.24
attributes attestation token

digitally signed data structure issued by an Attribute server that contains natural persons' attributes and is intended to be consumed by a Resource Provider

Note to entry: An attributes attestation token is issued to a client application and contains attributes about a natural person, has a defined validity period and is intended to be consumed by one or more designated Resource Providers.

3.25
attribute provider
organization trusted by one or more natural persons and one or more Resource Providers to issue attributes related to a natural person

3.26
authoritative party
entity that has the recognized right to create or record, and has responsibility to directly manage, an attribute associated with an individual

Note to entry: Jurisdiction(s) and/or industry communities sometimes nominate a party as authoritative. It is possible that such a party is subject to legal controls.

[SOURCE: ISO/IEC TS 29003:2018 Information technology — Security techniques — Identity proofing]

3.27
claimed PII
PII as claimed by a PII principal

3.28
client application
piece of software/hardware used by a user to interact with other remote components

3.29
community of interest
group of parties, member of a trust framework, who wish to obtain or verify an age determination attribute relating to a natural person

NOTE Members of a community of interest can include relying parties and age assurance services.

3.30
contra-indicator
evidence or pieces of information that call into question or otherwise indicate that an age determination attribute may not be correct

Note to entry: Contra-indicators can be at a natural person level, such as inconsistent information from multiple sources; or at a system level, such as a presentation attack or seeking to exploit a system vulnerability.

3.31
decision maker
organization or person responsible for making an age-related eligibility decision

Note to entry: An age-related decision maker could be an individual member of staff, a system or process, could be automated or require human intervention.

3.32
evidence
information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

[SOURCE: ISO/IEC 13888-1: 2009, 3.11]

Note to entry: Evidence does not necessarily prove the truth or existence of something, but can contribute to the establishment of such proof.

3.33
identifying attribute
attribute that contributes to uniquely identifying a natural person within a given context

3.34
identity
set of attributes which makes it possible to identify a natural person within a given context

3.35
identity information provider
entity that makes available identity information

Note to entry: Typical operations performed by an identity information provider are to create and maintain identity information for entities known in a particular domain. An identity information provider and an identity information authority may be the same entity.

[SOURCE: ISO/IEC 24760-1:2011, 3.3.4]

3.36
indicators of confidence
quantitative, qualitative or descriptive measure of the correctness and accuracy to which an age determination attribute can be stated to relate to a natural person

3.37
intermediate third party (ITP)
third party trusted by both a client application and a Resource Server to issue either security tokens or documents that contain a visible electronic seals (VES) which contain, among other information, an age determination attribute

3.38
linkability
property for a dataset where it is possible to associate an age determination attribute with the legitimate natural person

3.39
liveness
quality or state of being alive, made evident by anatomical characteristics, involuntary reactions or physiological functions, or voluntary reactions or subject behaviours

EXAMPLE 1: Absorption of illumination by the skin and blood are anatomical characteristics.

EXAMPLE 2: The reaction of the iris to light and heart activity (pulse) are involuntary reactions (also called physiological functions).

EXAMPLE 3: Squeezing together one's fingers in hand geometry and a biometric presentation in response to a directive cue are both voluntary reactions (also called subject behaviours).

[Source: ISO/IEC 30107-1:2016, 3.2]

3.40
liveness detection
measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture

[Source: ISO/IEC 30107-1:2016, 3.3]

3.41
metadata
data about data

[SOURCE: ISO 19115:2003, 4.1.26]

3.42
policy maker
governmental, regulatory, authorising organisation, corporation or person responsible for establishing age-related eligibility requirements for access to goods, content or services

Note to entry: A policy for age-related eligibility can be applied consistently across a jurisdiction or organisation or individually to a location, premises or provider of age-related goods, content or services through individually applied policy decisions, restrictions or permissions.

3.43
presentation attack
presentation to the age assurance system with the goal of interfering with the operation of the system

Note to entry: For Biometric Presentation Attack Detection see ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework, however, this standard also refers to documentary or record presentation attacks

3.44
primary credential
document or record from an authoritative party used that provides evidence of attributes associated with natural person

3.45
resource provider
organisation that makes a resource or service available online

[Source: ISO 24622-1:2015, 2.30]

3.46 resource server (RS)
server from an organisation that makes a resource, content or service available online

3.47
secondary credential
an attribute relating to a natural person derived from a primary credential

3.48
security token
digitally signed data structure issued by an ITP that contains users' attributes and is intended to be consumed by a Resource Server

Note to entry: a security token is issued to a client application and contains attributes about a user, has a defined validity period and can only be consumed by one or more Resource Servers.

3.49
set of indicators of confidence
non-structured list of indicators of confidence

3.50
social proofing
analysis, with a user's consent, of their digital footprint and the related social graphs, which can be interrogated to assess the veracity of a self-asserted age assurance claim

3.51
server application
application managed by a resource provider

3.52
trust
degree to which an entity has confidence that a product or system will behave as intended or degree to which a user or other stakeholder has confidence that a product or system will behave as intended

[Source: ISO/IEC 25010:2011, 4.1.3.2]

3.53
trust framework
set of requirements and enforcement mechanisms for parties exchanging identity information

[Source: ISO/IEC 29115:2013, 3.28]

3.52
unlinkability
property that ensures that a PII principal may make multiple uses of resources or services without others being able to link these uses together

[Source: ISO/IEC TR 27550:2019, 3.25]

3.53
untraceability
property that ensures that it is not possible to know which age assurance provider has issued a security token among a set of age assurance providers

3.54
user attribute
inherent property or characteristic of a user that can be distinguished quantitatively or qualitatively by a human or automated means

Note to entry: In the context of this document, a user is a natural person.

3.55
user notice
information given to a user in a concise, intelligible and easily accessible form about the goals of the processing of their PII

3.56
visible electronic seal

two-dimensional bar code included in a document that allows to check the authenticity and integrity of some data present in the document

4 Characterisation of Age Assurance Systems

4.1 Age Assurance Systems

An Age Assurance System shall consist of:

(a) One or more assurance components that indicate a natural person's age determination attribute
(b) A processing sub-system that analyses the indicators of confidence that can be applied to the assurance component(s) and communicate that to a relying party

Note: A general model as an option for the technical architecture for an age assurance system is provided in Annex A

4.1.1 Age assurance components

Age assurance components are established by capturing information from or about a natural person regarding:

(a) Something that they know about themselves or about others (such as their date of birth)
(b) Something that they possess, which is usually only possessed by persons of a known minimum age (such as a credit card)
(c) Something that they are or are inherent features about them (such as biometrics, behaviours or appearance)
(d) An attestation by a trusted third party (such as a parent or legal guardian)

Age assurance components establish age determination attributes or combine multiple sources together to elevate trust in the attributes associated with the natural person.

The assurance components may include:

(a) A claimed age attribute by the person – known as a self-asserted age attribute *Editor's Note: SC27/WG5 Experts did not reach a consensus on whether or not a claimed age attribute by the person can or should be considered an assurance component.*
(b) A process or system deriving an age determination attribute from an identity document from an authoritative source - for example an 18 plus determination attribute derived from the date of birth in a passport
(c) A process or system deriving an age determination attribute from primary or secondary credentials, a data set, a determination attribute attestation provider or identity service provider
(d) A process or system deploying artificial intelligence to ascertain age from one or more biometric identifiers, behaviours, characteristics or actions of individuals
(e) A process or system deploying social proofing to obtain or verify age determination attributes
(f) A process or system based on the attestation of trusted parties (such as parents or legal guardians) about the age of a person
(g) An assessment led by a trained human assessing elements that take into account a person's appearance, demeanour, background and credibility in person or online
(h) A process or system that derives age determination attributes from any other method that can establish indicators of confidence as described in this international standard

4.1.2 Primary and Secondary Credentials

Age Assurance Systems should take particular care with the difference between primary and secondary credentials.

A primary credential is a document or record issued by an authoritative party used by a natural person to provide evidence for some set of attributes. The authoritative party is an entity that has the recognized right to create a document or record, and has responsibility to directly manage, an identifying attribute. It could be a governmental agency, public body or a private body established for such purposes.

An Age Assurance System should consider a process for contra-indicators even when examining primary credentials. There is an inherent risk that the primary credential may have been issued inappropriately, to the wrong individual, with incorrect data on it, or may have been subject to falsification.

A secondary credential is an attribute relating to a natural person derived from a primary credential. It may be that the secondary credential is issued or handled by a reliable, trusted or authoritative source, but where it is derived from a primary credential, it should still be assessed for reliability. As an example, a bank may establish an account record from an authentication process involving capturing data from a natural person's passport. The examination by the bank of that passport is the examination of a primary credential. The creation of a record on the bank's system of the data about the natural person, is the creation of a secondary credential.

Age Assurance systems can rely on both primary and secondary credentials, but shall take additional risk assessed approaches to the handling of secondary credentials, including the capacity for data capture errors and the constraints, regulatory oversight and trustworthiness of the producer of the secondary credential.

4.1.3 Age processing sub-system

An age assurance processing sub-system may include:

(a) A process or system for gathering together assurance components from multiple sources
(b) A process or system for identifying attack vectors, protecting against presentation attack and assessing the liveness of individuals
(c) A process or system for identifying and addressing contra indicators
(d) A process or system for elevating the trust in an age attribute through multiple sources
(e) Facilities for individuals to exercise data rights
(f) A process or system for dissemination of age attributes, to a set of indicators of confidence, to relying parties
(g) A process or system for monitoring, continuously improving and learning from age assurance activities

4.2 Guidance for Policy Makers

A policy maker may determine the age-related eligibility requirements for access to some goods, content or services; the permitted age assurance solutions; the criteria to be met by the ITPs and any special provisions relating to the handling, storage and security of age and identity attributes by these ITPs; the appropriate entity authentication factors to be used by these ITPs.

A policy maker may implement the policy through legislative or non-legislative means, through permissions, authorisations or licensing requirements or through guidance or policy documents. A policy maker should consult relevant stakeholders and decision makers before establishing a policy and regularly review the policies to take account of societal and technological change.

A policy maker may remain agnostic of technological approaches or approve and regularly review certain particular technological approaches. A policy maker may also opt to specify approaches which are unsuitable, for instance deemed too easy to circumvent.

4.3 Categorization of Age Assurance solutions

4.3.1 Age verification

Age verification involves the use of a document bearing the identity and the date of birth of the natural person or sources of data about the natural person, where the age is computed using the time difference between the current date and the date of birth of the natural person without necessarily revealing the date of birth of the natural person to the provider of the service or a content.

Guidance: If such verification were done directly by the supplier of goods, content or services, it would necessarily acquire more information than strictly needed. The use of an intermediate third party allows to address that concern.

4.3.2 Age estimation

Age estimation involves the use of techniques where age determination attributes are estimated using inherent features or behaviours related to a natural person.

Such techniques may use the biometric characteristics of the natural person (e.g. his face and/or his voice) or information derived from his social behaviour (e.g. using social media data).

Age estimation is an approximation of the age and hence may provide a coarse granularity of age or of an age range.

Examples: Face analysis (e.g. using a short video) or voice analysis involves the use of artificial intelligence systems.

The presentation of a biometric spoof (e.g. a facial image or video of a person on a tablet or a fake silicone or gelatine fingerprint) to a biometric sensor can be detected by methods broadly referred to as presentation attack detection, PAD. ISO/IEC 30107-1 establishes a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed and communicated for subsequent decision making.

The analysis of social media data may also involve the use of artificial intelligence systems, but may simply involve the use of more classic algorithms such as keyword detection.

4.3.3 Age inference

Age inference involves the use of techniques where one or more age determination attributes can be inferred from the validity of a credential that provides information that allows the criterion to be tested.

Example 1: If marriage in a particular country is only permitted between individuals over the age of 16, and a valid government-issued marriage certificate is provided, that is sufficient evidence to allow verification that the named individuals are "over 16" or has been emancipated to the age of 16.

Example 2: If an attestation of trusted parties (such as parents or legal guardians) of a minor is produced and can be verified, then an age determination attribute for that minor can be derived from that attestation.

4.4 Age assurance practice statements

4.4.1 General

An age assurance provider shall document the operational practices and procedures utilised to provide assured age attributes.

A relying party shall document the acceptable approaches to age assurance that it adopts to comply with age-related eligibility decisions that it takes.

Note 1 A policy maker may determine the age-related eligibility requirement for access to goods, content or services; the permitted age assurance methodologies or solutions; any special provisions relating to the handling, storage and security of age and identity attributes; the independence of said checks from the relying party, whether it is appropriate to request an audit trail or not and any other specific measures the policy maker determines are appropriate.

Note 2 A policy maker may implement the policy through legislative or non-legislative means, through permissions, authorisations or licensing requirements or through guidance or policy documents. A policy maker should consult relevant stakeholders decision makers before establishing a policy and regularly review the policies to take account of societal and technological change.

Note 3 A policy maker may remain agnostic of technological approaches or approve and regularly review certain particular technological approaches. A policy maker may also opt to specify approaches which are unsuitable, for instance deemed too easy to circumvent.

4.4.2 Content of age assurance practice statements

An age assurance practice statement shall contain, as a minimum:

(a) The required outcome for the age-related eligibility decision identified (e.g. an under, over or between stated age eligibility requirements)
(b) A description of age assurance components utilised by the age assurance system, including:
    a. identifying the attribute sources (including whether or not they are an authoritative source);
    b. identifying whether or not they rely on primary or secondary credentials;
    c. if used, identifying the age verification systems being deployed to establish an age determination attribute
    d. if used, identifying the age estimation systems being deployed to establish an age determination attribute
(c) A description of the indicators of assurance necessary from the system or process in accordance with the vocabulary of this document
(d) A description of how the age assurance provider approaches protect the privacy of users in accordance with applicable laws, including the data protection laws and obligations, which shall include:
    a. how the age assurance system meets the privacy objectives in section 6 of this international standard
    b. how only the minimal amount of personally identifiable information is processed for the purpose of gaining the required indicators of confidence for age assurance to be established;
    c. how personally identifiable information gathered for the purpose of age assurance is limited to that purpose (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable);
    d. how the party will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made on the basis of inaccurate or incomplete data and addressing breaches in the security of that data
(e) A description of how the age assurance approaches offer functionality appropriate to the capacity and age of a child or adult who might use the service;
(f) A description of how the age assurance system addresses the security objectives in section 7 of this international standard;
(g) A description of how the age assurance provider seeks secure the use of the age assurance system in a manner that includes:

a. approaches that are accessible and inclusive to users with protected characteristics or additional needs
b. approaches that do not unduly restrict access of children or adults to services to which they should reasonably have access, for example, news, health and education services;
c. approaches that provide sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child or an adult

(h) A description of how the system, practice statement and approaches to age assurance system is kept under continuous and regular review, including by the Top Management of the organisation.

4.5 Acceptability of age assurance systems from the point of view of the individual

An individual shall be able to make his own opinion whether the solution fulfils the set of criteria that he believes to be necessary either from a privacy point of view or from a security point of view.

In order to help individuals to make their own opinion, each solution shall publicly disclose how/if the six privacy objectives are met and how/if the four security objectives are met in their age assurance practice statement.

4.6 Analysis of the ease of use from the point of view of the individual

If the age assurance system is not easy to use, either it will be rejected by the individuals or the individuals will attempt to circumvent it. From the perspective of individuals, the age assurance service provider shall identify the constraints to use the age assurance system.

5 Age determination attribute

A Resource Server (RS) may need to obtain an age determination attribute before the delivery of content, services or goods.

Within the class of age determination attributes, three types of age determination attributes may be requested by a Resource Server in order to be presented by a natural person to the Resource Server:

(1) over a certain age,

(2) under a certain age, and

(3) within an age range.

Examples: "> 16", "< 60" and "> 18 & < 30".

The first two types of age determination attributes can be modelled as a single-valued attribute while the third type can be modelled as a multi-valued attribute, where the first value indicates under which age the natural person should be and the second value indicates over which age the natural person should be.

When an attributes attestation token is used to convey a requested age determination attribute, that attribute should be present if the condition is met by the natural person and should be missing either if the condition is not met or if the Attribute Server is unable to provide a response to the request.

In this way, the Resource Server (RS) will be unable to make a difference between the case where the condition is not met and the case where the Attribute Server is unable to provide a response to that request, i.e. the case where the response is undefined.

6 Indicators of Confidence in Age Assurance

6.1 General

The indicators of confidence associated with an age determination attribute can be determined by the process deployed to capture, validate and verify that attribute in the age assurance system.

The indicators of confidence can be used by policy makers to set an age assurance policy.

A general scheme for indicators of confidence is provided at Annex A2.

6.1.1 Indicators of Confidence

Depending upon the underlying technique being used all Attribute Servers or an Age Assurance providers may not be able to deliver the three types of age determination attributes and not all values for each type.

When the age determination attribute is derived from the date of birth of the individual (i.e. in the area of age verification), an Attribute Server or an Age Assurance provider is able to respond to all the three types of age determination attributes and to any attribute value for each type.

An Attribute Server or an Age Assurance Provider using biometrics techniques may have only be trained to provide the attribute determination type "over a certain age" for individuals over 18 or within 12 to 18.

An Attribute Server or an Age Assurance Provider using specific documents to derive the age may only be able to provide the attribute determination type "over a certain age", e.g. for individuals over 18 or for individuals over 16.

This highlights the fact that indicators of confidence may be different upon the type of age determination attribute that is requested and the values that are requested by the Resource Server.

An Age Assurance System may support multiple indicators of confidence which are dependent upon the underlying technique being used.

6.1.2 Indicators of confidence for age verification systems

Since such systems are deriving the attribute determination attribute from the date of birth, they can support all the three types of age determination attributes and any attribute value for each type.

However, some indicators of confidence will be directly dependent upon the type of document that contains the date of birth, e.g. whether it is a primary credential or a secondary credential, whether an original or a photocopy of it is being used and the kind of verification that is performed on that document to verify both its origin and its genuineness. Three different indicators need to be considered.

The type of document being used may also depend upon the attribute value being checked; e.g. the same type of document will not necessarily be used for checking "Over 16" and "Over 60".

An Attribute Server and an Age Assurance Provider will need to refer to a different assurance policy depending upon the kind of checking being made.

That assurance policy will describe what is being done so that third parties (including policy makers) will be able to make their own opinion in the accuracy and reliability of specific age determination attributes and attribute value(s) and the set of indicators of confidence which are associated with them.

6.1.3 Indicators of confidence for age estimation systems

Such systems are usually deriving age determination attributes using artificial intelligence (AI) to ascertain an age from one or more biometrics characteristics.

Such systems first need to be trained using a set a data that is representative of the population that will be checked.

The set of data being used will be dependant upon the age range being checked, the colour of the skin and the ethnic origin.

Furthermore in order to increase the accuracy, different set of training data can be used for some types of age determination attributes and for some attribute values.

Biometrics systems using artificial intelligence (AI) exhibits both :

- a False Acceptance Rate (FAR): the percentage of identification instances in which persons that do not comply with the criteria are incorrectly accepted; and

- a False Rejection Rate (FRR): the percentage of identification instances in which persons that do not comply with the criteria are incorrectly rejected.

For a given biometric system, the crossover error rate (CER) is the point where the FAR crosses over with the FRR. A lower CER indicates that the biometric system is more accurate.

Beside the accuracy of the biometrics system, other factors need to be taken into consideration: the speed or throughput rate, and the acceptability to users.

Attribute Server and an Age Assurance Provider will need to refer to a different assurance policy depending upon the kind of checking being made.

That assurance policy will describe what is being done so that third parties (including policy makers) will be able to make their own opinion in the accuracy and reliability of specific age determination attributes and attribute value(s) and the set of indicators of confidence which are associated with them.

6.1.4 Indicators of confidence for age inference systems

Such systems are usually deriving age determination attributes using a document that provides information which indirectly allows to determine that a natural person is over a certain age.

As an example, the possession of a given type credit card may only be possessed by persons of a known minimum age.

However, the indicators of confidence will be directly dependent upon the type of document or the kind of object that is being possessed and the kind of verification that is performed on that document or object to verify both its origin and its genuineness.

The possession of one document or of one object only allows to make a check against a single attribute value.

If different type of documents or objects are being used the check will apply to different discrete values.

For each age determination attribute and for each attribute value, Attribute Servers and Age Assurance Providers will need to refer to a different assurance policy depending upon the kind of documents or objects being used and the checking being made.

7 Privacy objectives

7.1 Privacy Objectives for Age Verification Systems

The following privacy objectives have been identified:

7.1.1 Non-disclosure of the date of birth

The objective is to prevent Resource Servers (RS) to know the date of birth of the natural person. If this objective is supported, the date of birth of the natural person shall not be communicated by the Age assurance provider.

7.1.2 Non-disclosure of the age

The objective is to prevent Resource Servers (RS) to know the age of the natural person. If this objective is supported, the age of the natural person shall not be communicated by the Age assurance provider.

7.1.3 Unlinkability

The objective is to prevent Age Assurance providers from the ability to correlate transactions performed by the same individual on different services. If this objective is supported, the solution shall identify how this property is being obtained.

Guidance: If a security token is being used and if it contains a set of attributes allowing to uniquely identify the individual in any context, then this objective cannot be met. The same consideration applies when a visible electronic seal (VES) is being used.

7.1.4 Untraceability

When a third party is involved, the objective is to prevent the third party from knowing to which Age assurance provider the attributes (including age verification or age estimation) that have been placed into a security token will be presented by the individual. If this objective is supported, the solution shall identify how this property is being obtained.

Guidance: If a security token is being used and if it contains a field which allows to uniquely identify the target server, then this objective cannot be met. The same consideration does not apply when a visible electronic seal (VES) is being used.

7.1.5 Attributes minimisation

The objective is to restrict the amount of attributes disclosed by a individual to the minimum necessary to perform the transaction. If this objective is supported, the solution shall identify which attributes are being disclosed by the Age assurance provider.

Guidance: If a security token is being used, it should only contain an age verification or an age estimation attribute associated with one or more attributes allowing to link this security token to the legitimate individual. This objective cannot usually be met when using visible electronic seal (VES) generated in advance.

7.1.6 User Consent

The objective is to allow individuals to agree to communicate some of their attributes to a Resource Server (RS) through an affirmative process with the age assurance provider. Sufficient and meaningful information shall be provided to the individual so that they can understand, in a format and language that

can be reasonably expected to understand, which attributes will be released in the context of a given operation.

The individual should make his own opinion whether the requested age determination attribute is appropriate to be disclosed to the Resource Server (RS) that requests it.

As an example, asking for an attribute type "within an age range" with the attribute values 17 and 18, i.e. "> 17 & <18" would allow the Resource Server (RS) to know the date of birth of individual within one year.

The individual would need to make sure that such a request is really appropriate considering the type of service or good he is wishing to obtain from the Resource Server.

If this objective is supported, the solution shall identify how user consent is being obtained.

Guidance: The user consent should be obtained once the individual will have had the ability to take notice of the appropriate user notice.

Editor's Note: The SC27/WG5 Experts did not reach consensus about whether user consent should be required in all circumstances, pointing out that there are other potential lawful and proper bases for processing of personal data for the purpose of age assurance.

7.1.7 Transparency

The objective is to make sure that the attributes that have been placed into a security token are in accordance with the consent of the individual. If this objective is supported, the solution shall identify how this control is being done.

Guidance: The software used by the individual should be in a position to perform that verification and if the verification fails, should have the ability to stop the forwarding of the access token to the Resource Server.

7.2 Privacy Objectives for Age Estimation Systems

The objectives that apply to Age Verification Systems also apply for Age Estimation Systems. However, an additional objective applies.

7.2.1 Non-disclosure of biometrics characteristics

If biometrics characteristics are being used to estimate the value of an age determination attribute, the objective is to prevent Resource Servers (RS) to know the biometrics characteristics of the natural person.

Guidance: The use of an intermediate third party allows to address that concern.

7.3 Privacy Objectives for Age inference Systems

The objectives that apply to Age Verification Systems also apply for Age inference Systems. However, an additional objective applies.

7.3.1 Non-disclosure of the document or object being used

In such systems, a document or an object that provides information which indirectly allows to determine that a natural person is over a certain age is being used.

The objective is to prevent Resource Servers (RS) to know the exact content of that document or object related to the natural person.

For example, if a credit card is being used, the brand of the credit card should not be communicated.

Guidance: The use of an intermediate third party allows to address that concern.

8 Security objectives

8.1 Security Objectives for Age Verification Systems

The following four security objectives have been identified:

1. linkage of the attributes to the legitimate individual,
2. detection of collusion attacks between individuals
3. prevention of an endless usage of an evidence and
4. forwarding of a security token by an Age Assurance provider to another provider only if allowed.

8.1.1 Linkage of the attributes to the legitimate individual

In addition to the age determination attribute, the linkage should be done using one or more identifying attributes. If this objective is supported, the solution shall identify which identifying attribute(s) is/(are) being used or disclosed and how it/they will be used and verified by an Age Assurance provider.

Guidance: If a security token is being used, it should contain information allowing to link this security token to the legitimate individual. If that information is a set of attributes allowing to uniquely identify the individual, then the linkage will indeed be done but several privacy objectives will not be met: The same consideration applies when a visible electronic seal (VES) is being used .

8.1.2 Detection of collusion attacks between individuals

If two individuals agree to collaborate and one of them obtains an age determination attribute, and if that individual transmits that attribute to another individual, that other individual shall be unsuccessful to use it. If this objective is supported, the solution shall identify how this control is being done.

Guidance: A legitimate user, Bob, who has received from a security token that contains an age determination attribute stating that he is above a certain age (e.g. 18), might attempt to collaborate with another user, Alice, under a certain age (e.g. 13) in order to make believe to an Age assurance provider that the second user is above a certain age (e.g. 18) while in the real life reality Alice is under 13.

If such an attack is possible, it could be monetised and performed from anywhere: the two attackers do not need to be standing close together at the same location. The two attackers do not need to have any technical expertise: they only need to know how to use some software developed by some technical experts. They do not need to use high cost equipment: they simply need to know how to download on their usual terminal (e.g. a PC, a tablet or a smart phone) a specific software able to perform the attack.

8.1.3 Prevention of an endless usage of an evidence

The objective is to prevent the use of attributes contained in an evidence indefinitely.

Guidance: The evidence shall either be associated with an explicit or an implicit validity period or shall contain a challenge previously generated by the Ag Assurance Service Provider.

8.1.4 Forwarding of a security token by an Age assurance provider to **another Provider only if allowed**

If an Age assurance provider forwards to another Provider a security token that was intended to it, that other Provider shall be in a position to verify that the security token was effectively intended for itself. If this objective is supported, the solution shall identify how this control is being done.

Guidance: The security token should be targeted to one or more Age assurance provider so that each Provider can verify that the security token was targeted to itself. It is technically possible to target a security token to one or more Providers while supporting at the same time the untraceability objective.

8.2 Security Objectives for Age Estimation Systems

8.2.1 Biometric presentation attacks

Care should be taken to detect biometric presentation attacks. As an example, the liveliness of the individual must be checked so that still pictures, e.g. a still picture should be rejected.

Editor's Note: Additional text to be provided. Security objectives when using biometrics techniques may be different from security objectives when using social behaviour techniques.

8.3 Security Objectives for Age inference Systems

Editor's Note: Additional text to be provided.

9 Age Assurance Systems Attack and Contra-Indicators

9.1 General

Age Assurance providers shall recognise that their systems are vulnerable to attack – at a systemic level; when processing individual age assurance components; and when communicating age assurance outputs to relying parties.

Age Assurance providers shall take action to anticipate and address systems attack, presentation attack and the vulnerability of their systems.

9.2 Attack Vectors

Age Assurance systems should identify the attack vectors relevant to the security of the assurance component(s) selected to form a part of the system.

An attack vector is the path or means by which an attacker attempts to circumvent the age assurance process in order to obtain a malicious outcome.

These should consider:

(a) The accuracy, trustworthiness, fraud risk of the source of the data, including consideration of the risks associated with inferring or deriving data from other sources used for other purposes;
(b) The ease of scale of a system attack; whether or not a scalable attack can be monetised or programmable via remote activity, from anywhere;
(c) The ease for an individual to circumvent the system, including an assessment of the need for technical expertise, high cost equipment or repeatable;

(d) The ease for collusion and complicity between parties (including between children and their parents or legal guardians);
(e) The impact of system vulnerabilities on the confidence in the age assurance output generated

9.3 Contra-Indicators

Age Assurance systems may deploy multiple age assurance components and may have multiple sources of information from both primary and secondary credentials. These may lead to mis-matches of data or information indicating that the claimed age may not be the true age. These are called contra-indicators.

Age Assurance system providers have two options when presented with a contra-indicator:

(a) Take action to resolve the contra-indicator by gathering more evidence in support of the claimed age; or
(b) Communicate the existence of the contra-indicator to each relying party

Bibliography

[1] ISO #####-#, *General title — Part #: Title of part*

[2] ISO #####-##:20##, *General title — Part ##: Title of part*

A.1 Annex – General Model for Age Assurance Systems (Informative)

A.1.1 General Model

An age assurance system may also provide for a general model. In order to ease the description of the model, the following components are identified:

(a) one or more client applications: an application used by a natural person to access to the supplier of goods, content or services
(b) one or more Resource Servers (RSs): a server under the control of a supplier of goods, content or services.
(c) none, one or more intermediate third parties (ITP).

A.1.2 Intermediate Third Parties

When an intermediate third party (ITP) is being used, the ITP may:

(a) generate, upon the request from a client application and at the time the natural person is making a connexion with a supplier of goods, content or services, a security token which contains, among other information, an age determination attribute,
or
(b) may provide to individuals documents (e.g. PDF documents) that contain a visible electronic seal (VES) which contains, among other information, an age determination attribute.

A.1.3 Objectives for Resource Servers (RSs)

Editor's Note: ISO/IEC JTC1/SC27/WG5 – Identity Management and Privacy Working Group did not reach a consensus on whether or not the objectives for resource servers, intermediate third parties or client applications should be included or whether they go into too much detail about a particular system architecture for one type of solution. The text presented below to aid discussion and comments, was presented by an SC27/WG5 expert for inclusion in the working draft.

A.1.3.1 General

A Resource Server should support user consent.

A Resource Server shall be able to accept at least one age assurance solution, i.e. age verification, age estimation or age inference.. A Resource Server may use more than one age assurance solution, in particular when it exhibits different sets of indicators of confidence.

A Resource Server shall document the supported age assurance solution(s) that it adopts to comply with age-related eligibility decisions that it takes according to the goods, content or services that it supplies or makes available.

When a solution requires the use of one or more ITPs, the Resource Server shall indicate how to identify the ITPs that it trusts and how to verify the origin and the integrity of the access tokens generated by that ITP or a set of ITPs.

A.1.4 Contra-indicators and linkage of an age attribute

A.1.4.1 Contra-indicators

The use of multiple sources of information for age assurance may lead to mismatches of information between these sources. These mismatches are called contra-indicators.

When presented with a contra-indicator, a Resource Server should deny the access and communicate the existence of the contra-indicator either to the ITP, otherwise to its governing authority, when this is possible.

A.1.4.2 Linkage of an age attribute

When an ITP supporting an age verification process is being involved, the confidence in the verification made by the Resource Server between an age attribute and an individual is directly related to the relationship between the set of attributes already known to the Resource Server and one or more identifying attributes included into the security token.

The identifying attribute(s) included into the security token shall be compared with the set of user attributes already known by the Resource Server. The Resource Server shall then decide if the intersection between these two sets of attributes is sufficient or not to uniquely identify the user.

If the Resource Server decides that the intersection between these two sets of attributes is sufficient enough to uniquely identify a user, then the age attribute can be associated with the user account maintained by the Resource Server.

When the security token contains a single identifying attribute, several types of identifying attributes can be considered by the Resource Server:

(a) a globally unique user identifier (e.g. a personal email address, a social security number including the issuing country, a passport number including the issuing country c, a driving licence including the issuing state or country), or

(b) a locally unique user identifier used by the ITP to identify the user, whatever Resource Server is being involved (e.g. a single pseudonym used for all the servers), or

(c) a unique user identifier issued by the ITP to identify the user for each ITP / Resource Server pair (e.g. a different pseudonym for each ITP / Resource Server pair),

(d) a unique user identifier used by the ITP to identify the user for each individual / Resource Server pair (e.g. a different pseudonym for each individual / Resource Server pair), or

(e) a temporary user unique identifier used by the ITP to identify the user, that is only valid during a single session between the client and the ITP, whatever Resource Server is being involved (e.g. a large random number).

A.1.4.3 Globally unique user identifier

Several Resource Servers (not necessarily receiving a security token) may be able to establish a link between their users' accounts by using this single identifying attribute. In that case, the unlinkability property cannot be supported.

A.1.4.4 Locally unique user identifier

Several Resource Servers (receiving a security token from the same ITP) may be able to establish a link between their users' accounts by using this single identifying attribute. In that case, the unlinkability property cannot be supported.

A.1.4.5 User identifier unique for each ITP / Resource Server pair

In order to be able to generate such an identifying attribute, the client shall disclose to the ITP, an identifier of the Resource Server. This allows the ITP to know where the security tokens it issues are likely to be used.

This may be a concern in terms of privacy, since the ITP will be able to act as "Big Brother". However, several Resource Servers (receiving security tokens from the same ITP) will be unable to establish a link between their users' accounts by using this single identifying attribute. In that case, the unlinkability property will be supported but the untraceability property will not be supported.

A.1.4.6 Unique user identifier for each User/ Resource Server pair

Several Resource Servers (receiving a security token from the same ITP) will be unable to establish a link between their users' accounts by using this single identifying attribute. In that case, both the unlinkability property and the untraceability property will be supported.

A.1.4.7 Temporary unique user identifier

Several Resource Servers receiving security tokens from different ITPs will be unable to establish a link between their users accounts by using this single identifying attribute. However, the linkage of the security token with the legitimate individual may be weak and collusion attacks may be possible depending upon the implementation.

A.1.5 Objectives for intermediate third parties (ITPs)

An ITP may participate either in an age verification process, an age estimation process or an age inference process.

The ITP shall indicate how the security tokens or the electronic visible seals (EVS) it generates can be verified.

A.1.5.1 ITP supporting an age verification process

The ITP shall follow the requirements and guidelines provided in ISO/IEC 27701:2019.

The ITP shall use a document or a record about the individual issued by an authoritative party which is able to uniquely identify the individual and contains the date of birth of the individual. The authoritative party is an entity that has the recognized right to create or record, and has responsibility to directly manage, attributes associated with an individual. It may be a governmental agency, public body or a private body established for such purposes.

Care should be taken by the ITP to make sure that the attributes have not been issued inappropriately, to the wrong individual, with incorrect data on it, or may have been subject to falsification. (e.g. if using a fake driving licence, a doctored passport or a falsified record on a database).

Before the issuance of a security token, the ITP shall authenticate the individual. ISO/IEC 29115:2013 provides a framework for managing entity authentication assurance in a given context. The ITP shall position itself according to this framework.

The confidence for the inclusion of genuine attributes into a security token is directly related to:

(1) the strength of the authentication exchanges performed between the individual and the ITP,

(2) the nature of the verifications performed on the document issued by an authoritative party, e.g. a passport, an identity card or a driving license, while creating a user account,

(3) the nature of the verifications performed on additional documents, e.g. bills from a water company, an electricity supplier or a water supplier, while creating a user account, and

(4) the effectiveness of the security controls managed by the ITP to maintain the integrity of the user accounts.

The ITP shall document the operational practices and procedures utilised to create a user account and to deliver age determination attributes.

When inserting a visible electronic seal (VES) into a document, the ITP shall make sure that the user attributes contained in the VES are sufficient to enable Resource Servers to associate the VES to the legitimate individual.

A.1.5.2 ITP supporting an age estimation process

The ITP does not need to know the individuals. Facial analysis is to be distinguished from facial recognition: the aim here is to verify age, not to make a match with a database of photos of known individuals.

The ITP shall indicate and document the technique it is using.

Editor's Note: More text to be provided, but left to other contributors

A.1.5.3 ITP supporting an age inference process

The ITP shall indicate and document the technique it is using.

Editor's Note: More text to be provided, but left to other contributors

A.1.6 Objectives for client applications

From a privacy point of view, a client application should support both the user consent property and the transparency property.

From a security point of view, a client application should use mechanisms allowing to support the first three security properties.

A.2 Annex – Indicators of Confidence (Informative)

A.2.1 Indicators of Confidence in Age Assurance

An Age Assurance System may support multiple indicators of confidence. A scheme for indicators of confidence should be recognised in the jurisdiction, product category or service provision relevant to the use of an age related eligibility criteria.

An example of a scheme for indicators of confidence is provided in this Informative Annex.

Table 1 describes, in summary, five potential levels of confidence.

Table 1 – Schematic: Indicators of Confidence in Age Assurance

Asserted	Basic	Standard	Enhanced	Strict
• Based on self-asserted age attributes • No validation or trust elevation deployed • No attempt has been made to address contra indicators • Could be utilised in low risk or only where indicative age is required • Unlikely to be satisfactory for legally defined age-related eligibility	• Based on self-asserted age attributes with a single age assurance component that has low evaluation assurance level • Partial or simple validation or trust elevation; contra indicators may still be present • Could be used for unregulated age gateways	•Based on at least one age assurance component with standard evaluation assurance levels •Validated and all contra indicators addressed • Considered to be the minimum standard required for regulated age related eligibility unless a higher level is specified	• Based on two or more age assurance components with higher indicators of confidence and standard evaluation assurance levels • Validated and all contra indicators addressed • Likely to be useful for enhanced risk goods, content or services age-related eligibility	•Based on two or more age assurance components with higher indicators of confidence and higher evaluation assurance levels •Validated and all contra indicators addressed •Likely to be useful where age-related eligibility is critical to safeguarding or protecting the rights or freedoms of individuals

To achieve any given indicators of confidence, the age assurance process should meet at least each of the minimum requirements for that indicator. It may exceed the minimum in some dimensions but the indicators of confidence achieved are determined by the lowest achievement on any dimension.

A.2.2 Asserted Age Assurance

Asserted age assurance is the age claimed by the natural person by self-declaration or without the application of age assurance components. An asserted age can be captured in a data capture process, by reference to questions asked of the natural person or by historical assertion of age.

No attempt is made to validate the claimed age attribute.

An asserted age provides a low indicator of confidence that the age is assured to be the true age. An asserted age is not necessarily an incorrect age.

Asserted age assurance has validity at the time the attribute was claimed for a purpose where a low indicator of confidence is acceptable, but it has little value as a source of age assurance for future purposes. However, a change in a claimed age attribute by the same person may be a contra-indicator.

Note 1: In most cases, an asserted age is unlikely, by itself, to provide sufficient age assurance for regulated age-related eligibility decisions, but may be satisfactory for simple, low risk, user experience workflows in applications (such as where the user is merely being asked in what level of detail they would like information to be presented to them). The indicators of confidence can be increased marginally through technical measures, such as preventing repeat attempts at entering a date of birth or age, or not guiding the client by preventing the entry of an age which would make them ineligible.

A.2.3 Basic Age Assurance

Basic age assurance is the age claimed by the natural person by self-declaration with the application of at least one age additional assurance component.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of an age assurance component process.

The age assurance component process may include for the simple validation of the claimed age attribute.

An attempt may be made to reduce the attack vector from bots or automated processes and to prevent false or inaccurate self-declarations being made. This may include by establishing the simple liveness of a natural person. Such attempts should be supported by methods to reduce or eliminate systemic bias in the age assurance process.

A basic age assurance may still leave unresolved contra indicators – see s.8.6, which should be communicated to the relying party.

Basic age assurance should not be relied upon for more than two years.

Authentication should be renewed at least every 3 months.

A.2.4 Standard Age Assurance

Standard Age Assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least one age assurance component to validate the claimed age by reference to attributes related to the natural person.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of an age assurance component process.

The age assurance component process shall include for the validation of the claimed age attribute.

If the process is undertaken remotely, it shall include for the simple liveness of the natural person.

If the process involves a deployment of artificial intelligence, the classification or outcome error parity for protected characteristics for individuals shall be established.

The process shall include mechanisms to deter false or inaccurate self-declarations being made. An attempt shall be made to reduce the attack vector from bots or automated processes and to prevent false or inaccurate self-declarations being made. This may include by establishing the simple liveness of a

natural person. Such attempts should be supported by methods to reduce or eliminate systemic bias in the age assurance process.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

Standard age assurance should not be relied upon for more than one year, before it should be repeated to re-establish the validity of the age attribute.

Unless stated otherwise in an age-related eligibility policy, Standard Age Assurance shall be the age-related eligibility policy by default.

Authentication should be renewed at least every month.

A.2.5 Enhanced Age Assurance

Enhanced age assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least two other age assurance components from two independent sources (one of which shall be a primary or secondary credential) to validate the claimed age by reference to attributes related to the natural person.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of the age assurance component processes.

The age assurance component processes shall include for the validation of the claimed age attribute.

If the process is undertaken remotely, it shall include for the liveness of the natural person to be established in accordance with ISO/IEC 30107.

If the process involves a deployment of artificial intelligence, the classification or outcome error parity for protected characteristics for individuals shall be established.

The process shall include mechanisms to deter false or inaccurate self-declarations being made.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

Enhanced age assurance should not be relied upon for more than three months, before it should be repeated to re-establish the age attribute, or downgraded to standard age assurance.

Authentication should be renewed at least every week.

Note 1: Enhanced age assurance is likely to be useful for policy makers considering higher risk goods, content or services; where there may be a significant risk to the health, safety or wellbeing of individuals.

A.2.6 Strict Age Assurance

Strict age assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least two other age assurance components from two independent sources (one of which shall be a primary credential) to validate the claimed age by reference to attributes related to the natural person.

The age assertion can be captured in a data capture process by inviting the user to submit evidence in support of the age assurance component processes.

The age assurance component processes shall include for the validation of the claimed age attribute.

If the process is undertaken remotely, it shall include for the liveness of the natural person to be established in accordance with ISO/IEC 30107.

If the process involves a deployment of artificial intelligence, the classification or outcome error parity for protected characteristics for individuals shall be established.

The process shall include mechanisms to deter false or inaccurate self-declarations being made.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

Strict age assurance should repeated at each age-related eligibility decision, by repeating the age assurance process.

Note 1: Strict age assurance is likely to be useful for policy makers considering very high risk goods, content or services; or where seeking to safeguard the health, safety or wellbeing of individuals engaged in making or using very high risk goods, content or services.]

A.2.7 Combined Age Assurance Components

An age assurance provider may undertake an age assurance process that combines multiple assurance components to provide a higher overall indicators of confidence.

Table 2 shows an example scheme for combining multiple assurance components in a multi-level assurance scheme.

Table 2 – Schematic: Combinations of Assurance Components

To achieve:	Option 1	Option 2	Option 3	Option 4	Option 5
Standard Indicators of confidence	1 x Standard Age Assurance Component	2 x Basic Age Assurance Components	-	-	-
Enhanced Indicators of confidence	1 x Enhanced Age Assurance Component	2 x Standard Age Assurance Components	1 x Standard Age Assurance Component **PLUS** 2 x Basic Age Assurance Components	4 x Basic Age Assurance Components	-
Strict Indicators of confidence	1 x Strict Age Assurance Component	2 x Enhanced Age Assurance Components	1 x Enhanced Age Assurance Component **PLUS** 2 x Standard Age Assurance Components	1 x Enhanced Age Assurance Component **PLUS** 1 x Standard Age Assurance Component **PLUS** 2 x Basic Age Assurance Components	1 x Standard Age Assurance Component **PLUS** 4 x Basic Age Assurance Components