International Standard

ISO/IEC 27566-1

First edition
2025-12

Information security, cybersecurity and privacy protection — Age assurance systems —

Part 1: Framework

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de contrôle de l'âge —

Partie 1: Cadre de travail

Reference number
ISO/IEC 27566-1:2025(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with ITU-T (as ITU-T X.1901).

A list of all parts in the ISO/IEC 27566 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document sets out a framework and core characteristics for age assurance systems deployed for the purpose of enabling age-related eligibility decisions. These decisions can be made by anyone for any reason in any location through any type of relationship between an individual and the provider of any goods, content, services (such as the supply of alcohol, tobacco, weapons or online content), venues or spaces that have policy requirements for acquiring assurance about the age or age range of persons.

Age-related eligibility decisions are required when a person must either be a certain age, older or younger than a given age or be within an age range, where ages are counted in years and where these criteria are dependent upon the type of goods, content, services, venues or spaces provided.

This document aims to address issues associated with inadequately defined age assurance processes and associated lack of trust in terms of functionality, performance, privacy, security and acceptability. This document describes characteristics of an age assurance system to help policy makers, implementers and individuals understand and address the issues associated with deployment of age assurance systems.

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

The aim of this document is to enable policy makers (such as governments, regulators or providers of age restricted goods, content, services, venues or spaces) to specify applicable types of age assurance systems and associated indicators of effectiveness in their policy requirements.

As an example, a policy maker may determine that, to authorize the sale of alcohol or tobacco or some other age restricted product, a relying party acting as a decision maker should use a particular type of age assurance system supporting specified characteristics to verify that an individual is an adult.

This document does not:

— determine which type of age assurance system nor which type of age assurance method is appropriate for each type of age-related eligibility decision – that is a matter for policy makers;

— establish or recommend age thresholds for different goods, content, services, venues or spaces – these are matters for policy makers;

— deal with financial or commercial models for age assurance systems – these are matters for economic operators in the age assurance process;

— address the requirements for data protection for age assurance systems – these are matters for data controllers;

— consider age-related eligibility decisions based on parental controls or parental consent;

— consider age-related eligibility decisions based on testimonies from a trusted third party or established through a consent mechanism (such as a parent or legal guardian), since the documents that are required to be presented vary widely among different countries or even between different regions within a country.

Information security, cybersecurity and privacy protection — Age assurance systems —

Part 1: Framework

1 Scope

This document establishes a framework for age assurance systems and describes their core characteristics, including privacy and security, for enabling age-related eligibility decisions.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

3.1 Terms relating to age assurance

3.1.1
age assurance
set of processes and methods used to verify, estimate or infer the *age* (3.1.3) or age range of an *individual* (3.2.9), enabling organizations to make *age-related eligibility decisions* (3.1.9) with varying *degrees of certainty* (3.3.4)

3.1.2
age assurance result
information produced by an *age assurance system* (3.3.3) indicating that an *individual* (3.2.9) is a certain *age* (3.1.3), over or under a certain age or within an age range

3.1.3
age
number of complete years, months, days that have passed since the date of birth of an *individual* (3.2.9)

3.1.4
identity
set of attributes related to an entity

[SOURCE: ISO/IEC 24760-1:2025, 3.1.2, modified — notes to entry have been removed.]

3.1.5
identity document
physical or digital document issued by an *authoritative party* (3.2.6) containing identifying attributes

Note 1 to entry: This document can either have a physical form (plastic card, paper, etc.) or be immaterial (a collection of data cryptographically signed by an authoritative party).

Note 2 to entry: An identity document can be a *primary credential* (3.3.16) or a form of record of a *secondary credential* (3.3.17).

3.1.6
evidence
information supporting the occurrence of an event or action

Note 1 to entry: Evidence does not necessarily prove the truth or existence of something but can contribute to the establishment of such proof.

[SOURCE: ISO/IEC 13888-1:2020, 3.11]

3.1.7
age-related eligibility
qualification for access to goods, content, services, venues or spaces based on an age limit or an age band

3.1.8
age-related eligibility requirement
policy requirement for access to goods, content, services, venues or spaces based on an age limit or an age band

3.1.9
age-related eligibility decision
action by a *relying party* (3.2.2) to determine access to goods, content, services, venues or spaces based on an age limit or an age band

3.1.10
age verification method
age assurance method (3.3.2) based on calculating the difference between a verified year or date of birth of an *individual* (3.2.9) and a subsequent date

Note 1 to entry: In some cultures, an alternate calculation (such as use of birth year rather than birth date) can be applicable.

3.1.11
age estimation method
age assurance method (3.3.2) based on analysis of biological or behavioural features of humans that vary with age

Note 1 to entry: Such methods can use artificial intelligence (AI).

3.1.12
age inference method
age assurance method (3.3.2) based on verified information which indirectly implies that an *individual* (3.2.9) is over or under a certain age or within an age range

3.1.13
successive validation
type of age assurance process where multiple independent age assurance methods are used sequentially to establish an *age assurance result* (3.1.2)

3.1.14
practice statement
documentation of the practices, procedures and controls employed by an organization to fulfil a service

3.1.15
indicator of effectiveness
quantitative, qualitative, or descriptive measurement of the degree to which a given characteristic is achieved

3.1.16
inclusivity
capability of a product to be utilized by people of various backgrounds

Note 1 to entry: Backgrounds include (and are not limited to) people of various ages, abilities, cultures, ethnicities, languages, genders, economic situations, education, geographical locations and life situations.

[SOURCE: ISO/IEC 25010:2023, 3.4.6]

3.2 Terms relating to actors and parties

3.2.1
age assurance provider
entity responsible for providing *age assurance results* (3.1.2) to a *relying party* (3.2.2)

Note 1 to entry: The entity can be an organization providing an age assurance result to a relying party or an organization providing an application placed under the control of an individual and capable of deriving an age assurance result from a digital credential.

EXAMPLE A digital identity wallet is an example of an application placed under the control of an individual who is capable of deriving an age assurance result from a digital credential granted to the individual by a digital credential issuer.

3.2.2
relying party
entity that relies on an *age assurance result* (3.1.2) to make an *age-related eligibility decision* (3.1.9)

3.2.3
intermediary
entity that facilitates the interaction between *individuals* (3.2.9), *age assurance providers* (3.2.1), *relying parties* (3.2.2) and other parties to fulfil functions in an *age assurance system* (3.3.3)

EXAMPLE Digital credential issuers, credit agencies, mobile network operators or orchestration service providers.

3.2.4
policy maker
entity responsible for establishing *age-related eligibility requirements* (3.1.8) for access to goods, content, services, venues or spaces

Note 1 to entry: A policy maker can be:

a) external to the relying party, e.g. a governmental organization, a regulatory organization or authorizing organization, or

b) internal to the relying party.

Note 2 to entry: A policy for age-related eligibility can be applied consistently across a jurisdiction or organization or individually to a location, premises or supplier of age-related goods, content, services, venues or spaces through individually applied policy decisions, restrictions or permissions.

3.2.5
decision maker
organization or person responsible for making an *age-related eligibility decision* (3.1.9)

Note 1 to entry: An age-related eligibility decision maker can be an individual member of staff, a system or process or could be automated or require human intervention.

3.2.6
authoritative party
entity that has the recognized right to create or record, and has responsibility to directly manage, an identifying attribute

Note 1 to entry: Jurisdiction(s), industry communities or both, sometimes nominate a party as authoritative. It is possible that such a party is subject to legal controls.

[SOURCE: ISO/IEC TS 29003:2018, 3.3]

3.2.7
authoritative source
repository which is recognized as being an accurate and up-to-date source of information

[SOURCE: ISO/IEC 29115:2013, 3.5]

3.2.8
identity information provider
entity that makes available identity information

Note 1 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 can be the same entity.

[SOURCE: ISO/IEC 24760-1:2025, 3.3.4]

3.2.9
individual
human being, i.e. a natural person, who acts as a distinct indivisible entity or is considered as such

[SOURCE: ISO 29995:2021, 3.2.6]

3.2.10
consumer protection agency
governmental, state or non-governmental organization that aids consumers to protect their interests

3.2.11
sector association
not-for-profit organization in a specific sector made up of a collection of either companies or individuals, or both, with common interests

3.3 Terms relating to data and processes

3.3.1
age assurance component
part of an *age assurance system* (3.3.3)

3.3.2
age assurance method
process used to establish an *age assurance result* (3.1.2) to varying *degrees of certainty* (3.3.4)

3.3.3
age assurance system
system that utilizes one or more *age assurance methods* (3.3.2) to provide the *relying party* (3.2.2) with the necessary information to make an *age-related eligibility decision* (3.1.9)

3.3.4
degree of certainty
extent to which it is possible to be confident that a given fact is true

3.3.5
true positive
TP
correct measured value in positive results, that is, the case where both the measured and the correct results are positive

[SOURCE: ISO/TR 27877:2021, 3.1.4]

3.3.6
true negative
TN
correct measured value in negative results, that is, the case where both the measured and the correct results are negative

[SOURCE: ISO/TR 27877:2021, 3.1.5]

3.3.7
false positive
FP
incorrect measured value in positive results, that is, the case where the measured value is positive but the correct one is negative

[SOURCE: ISO/TR 27877:2021, 3.1.6]

3.3.8
false negative
FN
incorrect measured value in negative results, that is, the case where the measured value is negative but the correct one is positive

[SOURCE: ISO/TR 27877:2021, 3.1.7]

3.3.9
classification accuracy
percentage of the number of correct *age assurance results* (3.1.2) to the total number of age assurance results

Note 1 to entry: In this document, the classification is the likelihood that the age assurance system will produce a correct age assurance result.

3.3.10
attack vector
path or means by which one or more persons attempt to circumvent the *age assurance system* (3.3.3) in order to obtain a malicious outcome

3.3.11
contra indicator
information that calls into question or otherwise indicates that either an *age assurance result* (3.1.2) could be incorrect or that the *binding* (3.3.18) of the age assurance result to the right *individual* (3.2.9) could be incorrect, or both are incorrect

Note 1 to entry: Contra indicators can be at an individual 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.

3.3.12
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: An attack presentation can be a single attempt, a multi-attempt transaction, or another type of interaction with a subsystem.

[SOURCE: ISO/IEC 30107-3:2023, 3.1.1]

3.3.13
age analysis
correlation of behavioural and biological characteristics of humans that vary with age

Note 1 to entry: Age analysis is a process that does not involve the unique identification of any individual.

3.3.14
liveness
quality or state of being alive, made evident by anatomical characteristics, involuntary reactions, physiological functions, voluntary reactions, subject behaviours or any combination of these

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 30107-1:2023, 3.2]

3.3.15
liveness detection
measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine whether a biometric sample is being captured from a living subject present at the point of capture

Note 1 to entry: Liveness detection methods are a subset of presentation attack detection methods.

[SOURCE: ISO/IEC 30107-1:2023, 3.3]

3.3.16
primary credential
document or record from an *authoritative party* (3.2.6) that contains a set of attributes associated with the *individual* (3.2.9)

Note 1 to entry: A primary credential can either be physical (plastic card, piece of paper, etc.) or in electronic form (a collection of data signed by an authoritative party).

3.3.17
secondary credential
document or record relating to an individual derived from one or more *primary credentials* (3.3.16)

3.3.18
binding
property that relates an *age assurance result* (3.1.2) to the correct *individual* (3.2.9)

3.3.19
configuration management
activity of managing the configuration of an information system throughout its lifecycle

[SOURCE: ISO/IEC TR 10032:2003, 2.15]

3.3.20
digital footprint
information about an *individual* (3.2.9) that is captured because of their online activity or because of their interaction with some devices

3.3.21
fail safe
property of an *age assurance system* (3.3.3) that fails towards a safe *age assurance result* (3.1.2)

3.3.22
audit log
chronological sequence of audit records, each of which contains data about a specific event

[SOURCE: ISO 27789:2021, 3.9]

4 Overview of age assurance

4.1 Age

In this document, age is typically expressed as the number of complete years that have passed since the subject's date of birth. However, in certain cases, it can be necessary to specify age in days, months and years. This definition is intended to accommodate different legal and cultural practices of age representation, which can influence age-related eligibility decisions in various jurisdictions.

It can be necessary for a relying party to obtain age assurance before providing access to goods, content, services, venues or spaces. A relying party may request five types of age assurance results:

a) the actual age,

b) over a certain age,

c) under a certain age,

d) within an age range,

e) a culture specific indicator (such as one indicating a year of birth rather than a specific age).

EXAMPLE Where x denotes the age, "$x > 16$", "$x < 60$" and "$18 < x < 30$".

4.2 Characteristics of age assurance systems

This document establishes the characteristics of age assurance systems as described in Clauses 5 to 9. Figure 1 illustrates the structure of the framework.

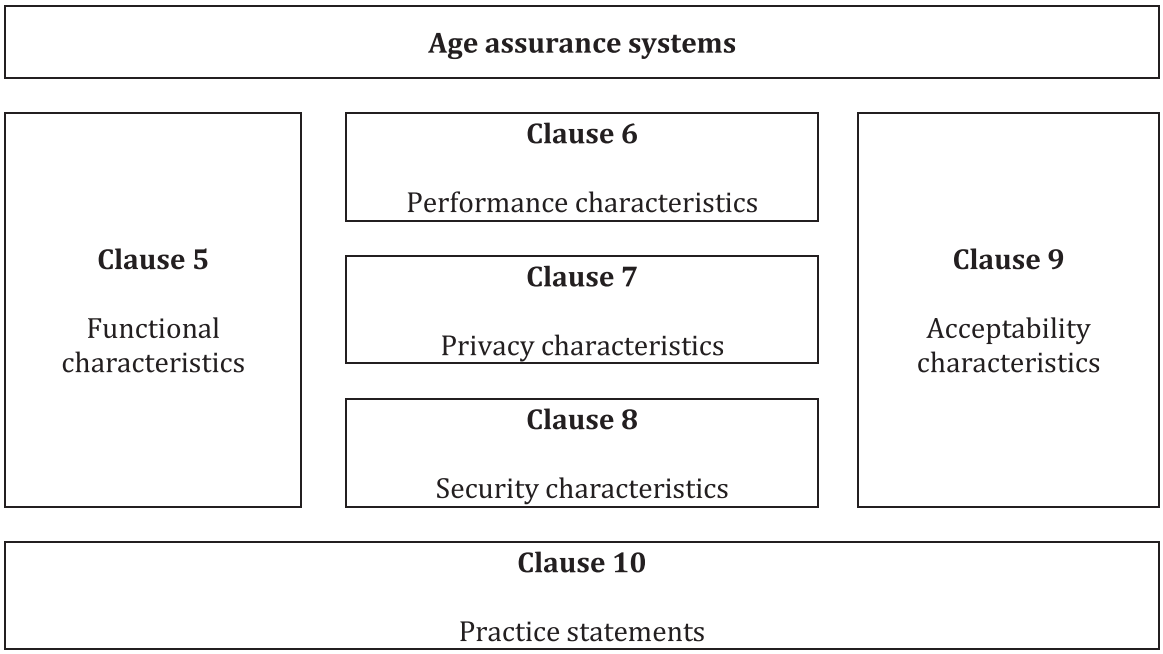

Figure 1 — Structure of the framework of age assurance systems

The characteristics described in this document form the basis for the approach by each entity involved in the age assurance process, be that of an age assurance provider, an intermediary or a relying party. Each entity should establish their process and provide a practice statement as described in Clause 10.

4.3 Age assurance methods

4.3.1 Overview of age assurance methods

This clause describes the three different age assurance methods, which when taken together with binding of evidence to the individual (see 5.3), can be used to generate an age assurance result leading to an age-related eligibility decision.

The age assurance methods recognized by this document include:

a) age verification methods;

b) age estimation methods;

c) age inference methods.

Figure 2 illustrates the three age assurance methods.

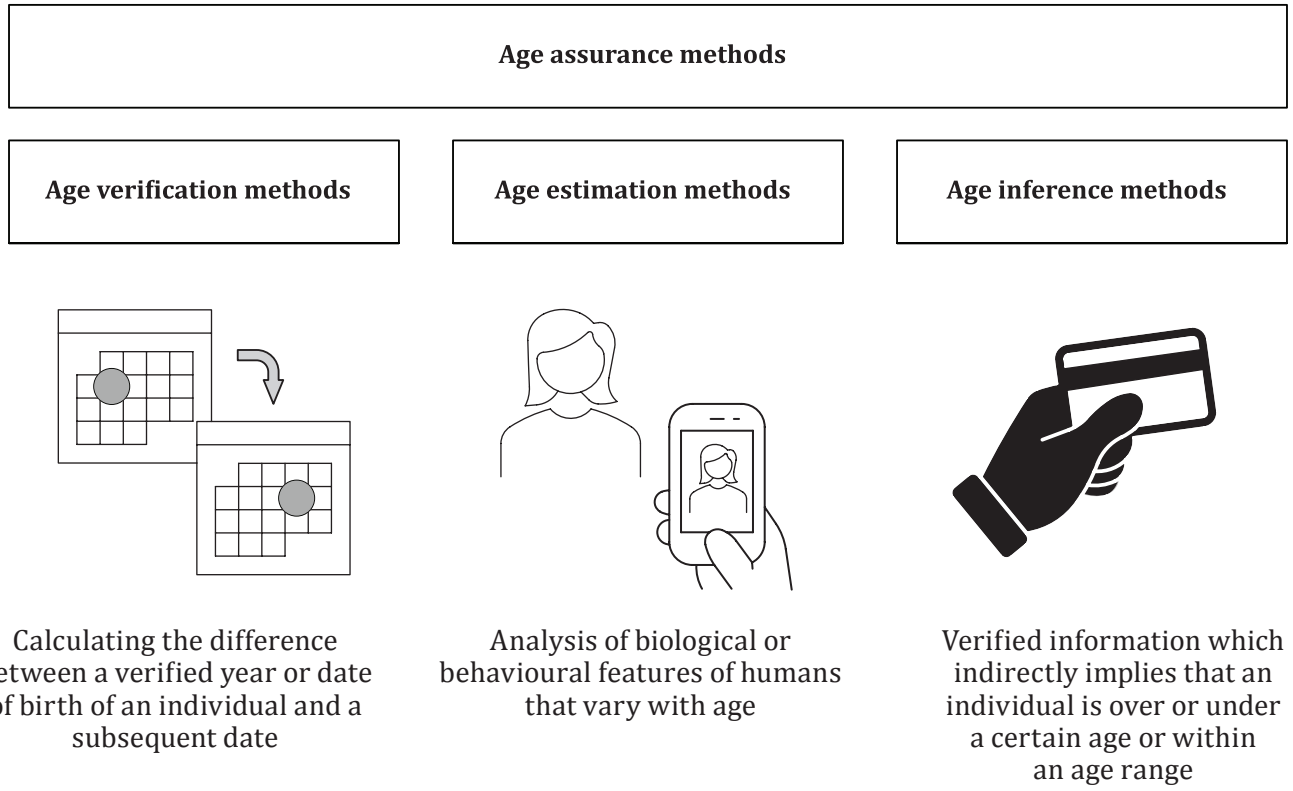

Figure 2 — Three age assurance methods

4.3.2 Age verification methods

Age verification methods typically use identity information from an identity document that includes the individual's date of birth. This process involves computing the difference between the date of birth in the document and a subsequent date to determine the individual's age on that date.

NOTE In some cultures, an alternate calculation (such as use of birth year rather than birth date) can be applicable.

Age assurance systems that use an age verification method shall ensure that the identity document:

a) is genuine;

b) is associated with the right individual;

c) is not expired;

d) has not been revoked nor suspended at the time it is used.

An age verification method can, for example, involve the use of an identity document bearing the date of birth of the individual or authoritative sources of data about the individual, where the age is computed using the time difference between the current date and the date of birth of the individual without necessarily revealing the date of birth of the individual to the provider of the goods, content, services or to the organization hosting venues or spaces. The age assurance provider should ensure that the credentials have not been issued inappropriately, to the wrong individual, with incorrect data on it or been subject to falsification (e.g. if using a fake driving licence, a doctored passport or a falsified record in a database).

If such verification had been done directly by the provider of goods, content, services, venues or spaces, it would necessarily acquire more information than strictly needed. The use of an age assurance provider allows that concern to be addressed, however it can also be mitigated by strict purpose limitation and data minimization within age assurance systems.

EXAMPLE 1 When an individual is seeking to access goods, content or services through the Internet and is using a smart phone, they can be prompted to provide a selective disclosure of attributes present in a digital credential stored in a digital wallet from the smart phone, where one of those attributes is indicating that they are over 18. The wallet can then compute a cryptographic proof demonstrating that they are over 18. That cryptographic proof can be communicated to the relying party.

EXAMPLE 2 When an individual is seeking to access a physical venue, they can use an application on a smart phone to establish a digital credential from verified evidence of their date-of-birth that they are over 18. They can then selectively share that information with a relying party through a one-time code (such as a 2D barcode) that contains cryptographic protection. That one-time code can be read by a device at the physical location (such as a kiosk or entry scanner) to enable access for the individual.

4.3.3 Age estimation methods

Age estimation methods involve the use of age analytics where age assurance results are estimated using inherent features or behaviours related to an individual that vary with age.

Such techniques can use age analysis to correlate the biological and behavioural characteristics of an individual (e.g. face, voice, hand geometry) or information derived from their behaviour (e.g. using social media data, email usage).

The analysis of behavioural data can involve the use of artificial intelligence systems but can also simply involve the use of techniques such as keyword detection.

EXAMPLE 1 When an individual is seeking access to services through the Internet, they can be asked to provide an image of their face, which can be subject to age analysis and liveness detection. The analysis can result in an indication that the individual is likely to be over 18. That age assurance result can be communicated to the relying party through a cryptographic proof.

EXAMPLE 2 When an individual is seeking access to online content and does not wish to disclose their identity or any identifying features, appropriate software can undertake age analysis of a non-identifying feature of humans that varies with age (such as dorsal hand geometry) and can estimate whether the individual who is presented is over 18. That age assurance result can be communicated to the relying party through a cryptographic proof.

EXAMPLE 3 When an individual is seeking to access a venue or spaces in a physical environment, a video camera can be placed at the entrance of the premises and when used with appropriate software can estimate whether the individual is over 18. A device linked to the camera can be used to indicate to the custodian of the premises that the individual is likely to be over 18 (or another age which the configuration settings can be adjusted to detect) or can indicate that another age assurance method is needed.

4.3.4 Age inference methods

Age inference methods involve the use of techniques where one or more age assurance results can be inferred from any evidence that provides information that allows the age of the individual to be implied.

Once it has been verified that these documents, information or devices are genuine and belong to the legitimate individual, a relying party can be reasonably confident that the legitimate holder meets either a minimum or maximum age requirement, or both, based on the content of these documents, information or devices, rather than using the date of birth directly.

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, it could be implied evidence to allow an age assurance result to be established that the named individuals are “over 16” or have been emancipated to the age of 16.

EXAMPLE 2 The possession of a credit card can indicate that a validated holder of that card (i.e. that they can authorize a transaction) is over the minimum age for issuance of such cards in the relevant jurisdiction.

4.3.5 Successive validation

Successive validation in age assurance involves using multiple methods to generate an age assurance result, enhancing accuracy and reliability. This approach sequentially applies different age assurance methods in consecutive order, such as an age estimation method, followed by an age verification method if insufficient effectiveness can be derived from the first check. By corroborating the age information through various independent methods, successive validation reduces the risk of errors and increases effectiveness in the age assurance process, ensuring enhanced effectiveness in the age assurance result.

4.4 Stakeholders

4.4.1 General

Stakeholders can be classified into the following non-exhaustive groups:

a) policy makers that enact age-related eligibility requirements for a given activity;

b) consumer protection agencies that take care of the interests of the individuals when considering age-related eligibility requirements issued by policy makers for a given commercial sector;

c) sector associations that defend the interests of providers of goods, content, services, venues or spaces.

4.4.2 Policy makers

Where a policy maker is external to the relying party, they can implement the policy through legislative or non-legislative means, through permissions, authorizations or licensing requirements or through guidance or policy documents.

Where a policy maker is internal to the relying party, in addition to age-related eligibility requirements imposed by legislation, it can voluntarily decide to enforce additional age-related eligibility requirements. As an example, the policy maker of a retailer can require that legally unrestricted goods should nevertheless be subject to voluntary restriction as a result of the ethical and community outlook that retailer decides to adopt.

A policy maker should consult relevant stakeholders before establishing a policy and regularly review the policies to take account of societal and technological change.

There is a possibility that a policy maker will either remain neutral to technological approaches or mandate the use of certain technological approaches. A policy maker may also identify approaches which are unsuitable, for instance deemed to be too easy to circumvent.

A policy maker should determine:

a) age-related eligibility requirements for access to goods, content, services, venues or spaces;

b) permitted age assurance methods;

c) criteria to be met by the relying party and other parties that can be involved in the age assurance system;

d) appropriate methods for binding of the age assurance result to the correct individual;

e) legal obligations or organizational commitments related to their practice statement.

4.4.3 Consumer protection agencies

There is a possibility that a consumer protection agency attempts to influence policy makers to improve the privacy of the consumers and act against companies that have unfair, deceptive and fraudulent business practices or break regulations or the law. They can also act against age assurance providers or relying parties that act contrary to their practice statements.

4.4.4 Sector associations

In the context of this document, the businesses that are members of a sector association are related to:

— providers of goods, contents services, venues or spaces subject to age-related eligibility requirements; or

— age assurance providers or intermediaries.

5 Functional characteristics

5.1 Age assurance systems

5.1.1 General

An age assurance system should be capable of meeting the stated needs of relying parties when it is used under specified conditions.

A functionally complete age assurance system comprises one or more age assurance methods selected or designed to provide the relying party with the necessary information to make an age-related eligibility decision.

The functional characteristics describe what a relying party, intermediary or age assurance provider is supposed to accomplish as set out in their practice statement (see Clause 10).

5.1.2 Age assurance providers

In order to avoid the unnecessary direct sharing of potentially personal data between the individual and the relying party, an age assurance provider acting as a third party can interact online between the individual and the relying party.

One of the age assurance provider's roles is to preserve the privacy of the individual towards the relying party by disclosing the minimum set of personal information and providing no more information than the relying party needs to know about the individual, if any. Its role can be to:

a) improve the cost effectiveness and efficiency of the age assurance system;

b) provide applications and services for users to provide evidence of age;

c) gather evidence from an individual to derive an age assurance result without communicating all of the evidence to support that result to the relying party;

d) serve as a third-party to provide security, privacy, redundancy or any other benefit to the age assurance system;

e) enable independent auditability, trust and confidence in age-related eligibility decisions.

An age assurance provider that provides a reusable age assurance result can require its users to have a user account on the provider's service before being able to provide the result to a relying party. This is the case when the age assurance provider stores evidence of age or a credential derived from an age assurance process for reutilization. This can include a process of binding an age assurance result to an individual through biometric comparison.

NOTE For more information about biometric comparison, see ISO/IEC 2382-37.

5.1.3 Intermediaries

Intermediaries are entities that can facilitate interactions among individuals, age assurance providers, relying parties and other stakeholders within the age assurance system. They can manage the exchange and validation of age-related information, data, security tokens or other information including making contributions to meeting the expected functional, performance, privacy, security and acceptability characteristics described in this document.

Intermediaries can play a role in streamlining the age assurance process and maintaining the confidence of all parties involved. They can support the implementation of age assurance measures, helping to ensure that age-related eligibility decisions are made reliably and according to applicable legal requirements and cultural practices.

Intermediaries can sit between the individual and the relying party or age assurance provider or between the age assurance provider and the relying party. They can be sources or repositories for age assurance components. When acting as an intermediary in a transaction, an entity cannot also be a relying party or an age assurance provider.

5.2 Data acquisition for age assurance components

5.2.1 Sources of data

Age assurance components can include (but are not limited to):

a) a process or system whereby an individual self-asserts their age (see 6.1.4);

b) a process or system deriving age from an identity document from an authoritative source, for example, an 18-plus indication derived from the date of birth in a passport;

c) a process or system deriving age from primary or secondary credentials, a data set, another age assurance provider or identity information provider;

d) a process or system that estimates probable age using age analysis;

e) a process or system using age analysis that derives from it an indication whether the individual meets an age-related eligibility requirement;

f) a process or system deploying age analysis from online activity of an individual;

g) a process or system inferring the age of an individual from the existence or possession of something age-specific;

h) a process or system whereby a person acting for a relying party assesses elements that consider the individual's appearance, demeanour, background and credibility in person or online;

i) a process or system that derives age assurance results from any other method.

5.2.2 Primary and secondary credentials

Age assurance systems should take particular care with the difference between primary and secondary credentials.

An age assurance system should consider a process for contra indicators even when examining primary credentials. There is an inherent risk that a primary or secondary credential has been issued inappropriately, to the wrong individual, with incorrect data on it or has been subject to falsification.

It is possible 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. An age assurance provider should also ensure trusted chains of sources of credentials. As an example, a bank may establish an account record from a process involving capturing data from an individual'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 individual is the creation of a secondary credential.

Age assurance systems can rely on both primary and secondary credentials but should 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.

5.2.3 Date transposition errors

Age assurance systems shall be capable of interpreting date information correctly.

Care should be taken to understand differing date formats in different countries on different documents.

EXAMPLE A date of birth expressed as 05/09/2010 can be 5 September 2010 or May 9 2010 depending on local date format custom and practice. According to the ISO 8601 series, the date is expressed as 2010–09–05 (yyyy-mm-dd) providing for effective interoperability. A failure to correctly transpose dates can result in an incorrect age assurance result.

NOTE Further guidance about handling dates can be found in ISO 8601-1.

5.3 Binding of age assurance result to the correct individual

5.3.1 Binding characteristics

Age assurance systems shall ensure that the age assurance result is accurately bound to the correct individual.

Appropriate measures shall be taken to prevent use of an age assurance result relating to one individual by any other individual. The ease for individuals to circumvent the system, including the need for technical expertise, high cost equipment or repeatability should be considered.

5.3.2 Approaches to binding

Some examples of approaches to binding include:

a) a unique identifier binding where the age assurance result is bound to the individual using a unique identifier. This identifier should be securely generated and managed to reduce the risk of duplication, misuse, disclosure or inadvertently adding to the individual's digital footprint. However, if two relying parties receive the same unique identifier, they can identify that the age assurance result relates to the same individual;

b) biometric binding where the system utilizes biometric data (such as facial recognition, fingerprinting. etc.) to ensure the data source or credential and the age assurance result are linked to the correct individual;

c) multi-factor binding which can include a combination of something the user knows (password), something the user has (token) and something the user is (biometric);

NOTE Further guidance on binding is available in ISO/IEC 29115.

d) key binding where the age assurance result is bound to a cryptographic key managed by a trusted application that is known to be resistant to collusion between collaborative individuals.

5.4 Age assurance data processing

An age assurance system can include a process or system for:

a) gathering together age assurance components from multiple sources;

b) identifying attack vectors (see 8.3.2), protecting against biometric presentation attack (8.3.3), spoofing attacks (8.3.4) and counterfeiting attacks (8.3.5);

c) identifying and addressing contra indicators (see 8.4);

d) elevating the trust in an age assurance result through multiple sources;

e) providing a source of trust for attestations, authoritative sources, etc.;

f) individuals to exercise data rights;

g) dissemination of indicators of effectiveness to relying parties;

h) monitoring, continuously improving and learning from age assurance activities;

i) storing credentials, attestations or age-related evidence, either using a client application or an online service;

j) monitoring and logging the activities and results of the system;

k) providing transparency reporting to authorized entities (e.g. regulators, auditors, certification bodies, researchers or to the public);

l) developing and publishing age assurance practice statements (see Clause 10) in appropriate human readable and machine-readable formats.

5.5 Configuration management

Upon request, the age assurance provider shall communicate to the relying party under agreed terms and conditions the standard configuration settings of the age assurance system.

Upon a request from a relying party, some specific configuration settings may be negotiated between the relying party and the age assurance provider.

The configuration settings should specify:

a) the availability, if any, of configuration settings for the age assurance system;

b) the impact of variable configuration settings on:

   1) the functional characteristics of the age assurance system,

   2) the performance characteristics of the age assurance system,

   3) the privacy characteristics of the age assurance system,

   4) the security characteristics of the age assurance system,

   5) the acceptability characteristics of the age assurance system;

c) the responsibilities and authorities of the parties to affect the configuration settings;

d) the approach to configuration management planning, change control, evaluation, disposition of change, configuration status accounting, documented configuration information and configuration audit.

NOTE Approaches to configuration management are available in ISO 10007.

5.6 Context in use

The contexts in which an age assurance system can be used shall be documented and a summary description shall be included in practice statements.

The system should enable individuals to complete the age assurance process successfully and consistently. They should be user-friendly, with intuitive interfaces that require minimal effort to navigate and understand.

The system should be adaptable to different contexts of use, including various cultural, legal and operational environments and as described in practice statements.

The system can provide for selection and choice by the user over different age assurance methods to be used.

Regardless of whether age is being established to restrict access to online content or services, access to spaces and venues or the ability to purchase physical goods, an age assurance system can include components or methods which are online or offline in any combination. This document does not provide guidance on which system designs are appropriate in different contexts.

5.7 Delivery of age assurance result

Age assurance systems shall implement secure delivery methods so that the delivery of an age assurance result from the age assurance provider to the relying party adequately mitigates confidentiality and integrity risks, and can be relied upon by the relying party.

6 Performance characteristics

6.1 Performance effectiveness

6.1.1 General

An age assurance system should perform effectively and with measurable consistency.

Table 1 illustrates a matrix that describes classification of age assurance results.

Table 1 — Confusion matrix in the case of a binary classification of age assurance results

		Age assurance result	
		Positive: over threshold	Negative: under threshold
Actual age	Positive: over threshold	True positive (TP)	False negatives (FN)
	Negative: under threshold	False positive (FP)	True negatives (TN)

6.1.2 Effective age assurance systems

An age assurance system that performs effectively shall:

a) cause a relying party to grant access to goods, content, services, venues or spaces for an individual who meets the criteria for age-related eligibility [known as a true positive (TP)]; or

b) cause a relying party to refuse access to goods, content, services, venues or spaces for an individual who does not meet the criteria for age-related eligibility [known as a true negative (TN)].

6.1.3 Ineffective age assurance systems

An age assurance system that fails to perform effectively can:

a) cause a relying party to grant access to goods, content, services, venues or spaces for an individual who does not meet the criteria for age-related eligibility [known as a false positive (FP)]; or

b) cause a relying party to refuse access to goods, content, services, venues or spaces for an individual who does meet the criteria for age-related eligibility [known as a false negative (FN)].

6.1.4 Use of self-asserted age

Self-asserted age (or self-declaration) is the practice of asking an individual to state their age.

EXAMPLE Self-asserted age involves circumstances when an individual is asked to:

— state their own age,

— tick a box to agree that they are a certain age, over or under a certain age or between an age range, or

— accept terms or conditions requiring them to meet an age-related eligibility criteria,

without that individual having to do anything else as a part of the age assurance system.

Self-asserted age may be included as part of an age assurance system, such as in a successive validation process.

An age assurance system that relies solely upon self-asserted age shall be considered ineffective for the purpose of making an age-related eligibility decision, which involves granting access to age-restricted goods, content, services, venues or spaces.

NOTE Self-asserted age can improve the delivery of age-appropriate information and experiences, such as news, health information, product instructions, explanatory information and transparency about age assurance.

6.1.5 Other factors affecting effectiveness

An age assurance system that performs effectively shall:

a) provide a low spread of errors that is consistent over different demographics (known as outcome error parity; see 6.3.3),

b) provide an age assurance result that relates to the individual in question (known as correct binding; see 5.3),

c) allow acquisition, processing and controls that adhere to the functional characteristics set out in this document (see Clause 5),

d) manage data in a manner that adheres to the privacy characteristics set out in this document (see Clause 7),

e) establish the system such that it adheres to the security characteristics set out in this document (see Clause 8),

f) operate in a manner that adheres to the acceptability characteristics set out in this document (see Clause 9).

6.2 Indicators of effectiveness

Indicators of effectiveness can be used to measure the degree to which a given characteristic is achieved, such as a functional, performance, privacy, security and acceptability characteristic. By employing these indicators, stakeholders can assess the reliability and robustness of the age assurance process, ensuring it aligns with relevant standards and regulations.

These measures provide transparency and build trust in the system's ability to enable age related eligibility decisions while safeguarding individual privacy and security.

An indicator of effectiveness can apply in particular to:

a) the classification accuracy of an age assurance result,

b) the binding of an age assurance result to the right individual, i.e. its correctness.

Policy makers can use the indicators of effectiveness to contribute to an age assurance policy (see 4.4.2) including granularity of the performance effectiveness of an age assurance system.

This document does not establish the labelling or categorization of the indicators of effectiveness.

6.3 Performance metrics

6.3.1 Classification accuracy

For each configuration of an age assurance system, the classification accuracy shall be determined, recorded and regularly reviewed.

The classification accuracy shall be stated in practice statements. This can include input parameters that affect the classification accuracy, such as configuration settings.

The classification accuracy should be expressed as a percentage.

The classification accuracy can be used to demonstrate indicators of effectiveness.

6.3.2 Primary metrics

The age assurance system should measure and report the false positive rate (FPR), defined as the percentage of incorrect positive classifications out of all actual negatives. This metric indicates the likelihood of incorrectly identifying individuals as meeting an age-related eligibility when they do not.

The age assurance system should measure and report the false negative rate (FNR), defined as the percentage of incorrect negative classifications out of all actual positives. This metric indicates the likelihood of failing to identify individuals who meet an age-related eligibility.

The age assurance system may measure and report on other secondary metrics where they are relevant to the method of age assurance. They can be useful for relying parties understanding the consequences of implementation of age assurance systems.

6.3.3 Outcome error parity

Outcome error parity in the context of age assurance refers to the principle that the system should provide consistent and fair error rates across different demographic groups. This means that the likelihood of false positives (incorrectly granting access) and false negatives (incorrectly denying access) should be similar regardless of the user's gender, ethnicity or other demographic factors. Achieving outcome error parity ensures that the age assurance system is unbiased and treats all users equitably, thereby enhancing the reliability and trustworthiness of the system.

6.3.4 Performance efficiency

The age assurance system should measure and report the average and maximum response time for processing age assurance requests, ensuring that it meets the performance requirements of the relying party.

The age assurance system should measure and report throughput, defined as the number of age assurance requests processed per unit of time. This metric assesses the system’s capacity to handle high volumes of requests.

The age assurance system shall evaluate and report its scalability, including how performance metrics (e.g. response time, throughput) are affected as the load increases. Scalability testing should simulate different load conditions to ensure the system performs reliably under varying demands.

The age assurance system should measure and report the completion rate of the age assurance methods utilized, indicating the percentage of users who successfully complete the process compared to those who initiate it.

6.4 Resource utilization

The age assurance system should optimize the use of computational resources, including processing power, memory and storage, to ensure efficient and sustainable operation.

The system should minimize resource consumption while maintaining the required performance, accuracy and security standards.

6.5 Testability

The age assurance system shall be testable.

This can include predefined test points, automated test frameworks, support for standard test tools and frameworks and deployment-specific tests including boundary and edge case validation.

7 Privacy characteristics

7.1 General

Privacy is paramount for age assurance systems to protect sensitive user information and build trust and confidence. These systems often handle personal data, including biometric information, which require robust safeguards to prevent misuse and unauthorized access. Ensuring privacy helps maintain user trust, which is essential for the adoption and effectiveness of age assurance technologies.

7.2 Privacy by design and default

Age assurance providers, intermediaries and relying parties should take a proactive approach that embeds privacy into the development and operation of age assurance systems from the outset and throughout their lifecycle.

The key principles include the following.

a) Privacy should be proactive, not reactive. Age assurance providers, intermediaries and relying parties should integrate privacy considerations into the design phase of the age assurance system to anticipate and prevent privacy risks before they occur, and they should conduct regular privacy impact assessments to identify and mitigate potential privacy risks.

b) The configuration settings should be established with the more privacy preserving option selected by default to ensure that personal data are automatically protected in any system or business practice and by default, no action is required by users to protect their privacy (see 5.5).

c) Privacy should be embedded into the architecture of the age assurance system, ensuring it is an integral part of the system's core functionality, including incorporating strong encryption and anonymization techniques to protect personal data throughout its lifecycle.

d) Ensuring that the data are protected throughout its entire lifecycle, from collection to processing, storage and eventual deletion, including through secure data transmission protocols, access controls and regular security audits.

e) Age assurance providers, intermediaries and relying parties should maintain transparency about data practices, allowing users to understand how their data are used, stored and protected, including through clear explanations in practice statements (see Clause 10).

NOTE Further guidance of the development of privacy by design can be found in ISO 31700-1.

7.3 Data minimization

7.3.1 Collection limitation

Age assurance systems shall collect only the minimum amount of personal data necessary for the purposes of establishing an age assurance result to the required degree of certainty by a policy maker.

7.3.2 Non-disclosure of age-related data

When providing the age assurance result to the relying party, the age assurance provider should not:

a) disclose the date of birth of the individual;

b) disclose the specific age of the individual based on a single request unless it is specifically required by the relying party (e.g. though a legal requirement or a specific regulation);

c) disclose the information used to infer the age of an individual;

d) disclose the physical appearance or characteristics of an individual.

7.3.3 Compliance with legal obligations

Age assurance providers should only disclose age-related data where the relying party can demonstrate a specific requirement in order for them to be able to comply with a legal obligation.

7.3.4 Purpose limitation

Age assurance providers and relying parties shall limit the acquisition of data for the purpose of age assurance solely to the creation of an age assurance result.

Age assurance providers and relying parties shall prevent data that has been gathered for the creation of an age assurance result from being used for onward purposes without explicit user consent.

7.3.5 Access control

Age assurance providers and relying parties shall implement strict access controls to ensure that only authorized personnel can access personal data including through the use of role-based access controls and the regular review of access permissions.

7.3.6 Data disposal

Age assurance providers and relying parties shall delete personal data when an age assurance result has been established and only retain the minimum amount of data necessary (such as anonymized transaction logs) to provide for charging for their services (if applicable).

NOTE 1 Legal requirements for retaining personal data can apply and are expected to be clearly explained in a practice statement.

NOTE 2 This clause is related to the collection minimization principle specified in ISO/IEC 29100.

7.4 Avoidance of adding to digital footprint

Age assurance systems should be structured so that they do not add information to an individual's digital footprint.

In particular, the following characteristics should be considered:

a) whether an implementation allows age assurance providers and relying parties to correlate transactions performed by the same individual on different services;

b) whether two or more collaborating relying parties are capable of knowing that access came from the same individual;

c) whether a third party can know from which age assurance provider an individual has obtained an age assurance result;

d) whether providers of age-related information or intermediaries can know by which relying party the age-related information may be used or has been used;

e) when the data are retained, such as for audit logs (see 7.6), whether anonymization or pseudonymization techniques have been applied immediately after an age assurance result is provided, preventing tracking and identification;

f) whether age assurance providers, intermediaries and relying parties minimize the flow of personal data through central servers;

g) whether personal data or biometric data related to an individual, if any, are deleted immediately after an age assurance result is provided or used,

h) whether single-use tokens can link back to an individual's identity.

7.5 User awareness

Age assurance providers and relying parties should ensure that individuals have sufficient awareness, through the publication of practice statements (see Clause 10) of the process of age assurance. Sufficient and meaningful information should be provided to the individual so that they can understand, in a format and language that they can be reasonably expected to understand, what data will be released to the relying party in a given context, and so that they can give, if applicable, their informed consent.

Where a relying party is seeking to deploy age assurance measures to prevent and detect criminal behaviour, such as child sexual exploitation and abuse, a relying party may determine that user awareness of the technique(s) used to achieve that objective would be counterproductive. In such cases, a relying party practice statement may exclude such technique(s) from user awareness, but they should, nevertheless, maintain a record of the processing activity and ensure an appropriate evidential chain for audits about the deployment of such technique(s).

NOTE Legal requirements can apply.

7.6 Audit logs

An age assurance component should maintain an audit log of all actions performed within the process.

Relying parties shall maintain an audit log of all access granted. They may maintain an audit log of all access denied.

These audit logs shall be integrity protected and retained for a period stated in practice statements.

The audit log shall not contain any biometric image or copies, images or data extracted from any identity document or record of any individual.

8 Security characteristics

8.1 Security by design and default

Age assurance providers, intermediaries and relying parties should take a proactive approach that embeds information security into the development and operation of age assurance systems from the outset and throughout their lifecycle. The key principles include:

a) incorporating security considerations into the initial design phase of the age assurance system to anticipate potential threats and prevent security breaches;

b) conducting regular threat modelling and risk assessments to identify and address security vulnerabilities early in the development process and throughout the system lifecycle;

c) designing the system architecture with security as a core component, using secure coding practices and following industry best practice for secure software development;

d) ensuring that the system's architecture includes strong encryption methods for data at rest and in transit to protect sensitive information;

e) implementing a multi-layered security approach, including firewalls, intrusion detection/prevention systems and secure access controls, to protect the system at different levels, including using defence-in-depth strategies to provide multiple layers of protection against various types of system attacks;

f) implementing continuous monitoring of the system for security threats and vulnerabilities, using automated tools and manual audits to detect and respond to potential issues promptly;

g) ensuring that all changes and updates to the age assurance system are traceable, allowing for easy identification of affected components;

h) developing and maintaining an incident response plan to ensure a rapid and effective response to security breaches or other security incidents.

NOTE Further guidance on the development of security by design can be found in ISO/IEC TS 19249.

8.2 Replay, forwarding or reuse of age assurance result

8.2.1 Replay of an age assurance result

An age assurance result shall be protected from unplanned reuse.

This ensures that the relying party can be confident that the age assurance result is current and not a replay of a previous message. When an age-related cryptographic digital proof is presented, in order to prevent replay, it shall include either a time variant parameter generated by the application used by the individual that has a negligible chance of repeating or a challenge previously generated by the relying party. This measure guarantees that the age assurance is timely and accurate, maintaining the integrity of the age-related eligibility decision.

8.2.2 Forwarding of an age assurance result

An age assurance result shall be protected from an unintended forwarding between relying parties. This helps to ensure that a relying party cannot reuse a result it has received to gain access to another relying party.

8.2.3 Planned memorization or reuse of an age assurance result

A relying party can memorize an age assurance result. If the same individual makes a subsequent request to the same relying party, they may use the memorized age assurance result instead of repeating the age assurance process. In that case, the relying party shall determine the appropriate duration for memorizing the age assurance result.

If an age assurance provider is able to bind an age assurance result to an individual (see 5.3), it can memorize the result, so that it can be used for the same or a different relying party.

8.3 Resistance to attack

8.3.1 Preparation for attack

Age assurance systems shall be designed and managed to be resistant to attack.

Age assurance providers should recognize that their systems can be vulnerable to attack:

a) at a systemic level;

b) when processing individual age assurance components, and

c) when communicating age assurance results to relying parties.

Age assurance providers should take action to anticipate and address systems attack and the vulnerability of their systems.

Age assurance providers should not be required to disclose their mechanisms to prevent attack vectors in their practice statement.

8.3.2 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.

Age assurance providers should consider:

a) the accuracy, trustworthiness and 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 a scalable attack can be monetized 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 repeatability;

d) the ease for collusion and complicity between parties, including individuals;

e) the impact of system vulnerabilities on the effectiveness of the age assurance result generated.

8.3.3 Biometric presentation attacks

An age assurance system shall be protected from biometric presentation attacks.

As an example, the liveness of the individual should be checked so that still pictures, replayed videos or use of 3D masks are rejected.

Biometric presentation attacks can be countered using either passive or active liveness detection.

Passive liveness detection does not require any specific action from the user. It analyses an individual's face in real-time to detect liveness using involuntary and reflexive signals, head and eye movements like blinks or other cues (e.g. using context cues and texture cues in the image to determine whether it is a person or an image in front of the camera).

Active liveness detection requires individuals to perform specific actions (such as eye blinking, head tilting, turning or smiling at a specific moment) on request in an order that changes for every liveness check. However, this test is more intrusive and time consuming than passive liveness detection.

NOTE Further guidance on biometric presentation attack detection can be found in ISO/IEC 30107-1.

8.3.4 Spoofing attack

An age assurance system shall be protected from spoofing attacks.

A spoofing attack is a specific attack vector when an individual is attempting to fool the age estimation method, e.g. by trying to look older than they really are by wearing a hat, glasses, a fake beard or a fake moustache.

8.3.5 Counterfeiting attack

An age assurance system shall be protected from counterfeiting attacks.

A counterfeiting attack is a specific attack vector when an individual presents an identity document that is either not genuine, or its origin cannot be appropriately verified, or both.

Validation of that document is important for the chain of trust. The persons or systems undertaking the validation shall be trained depending upon the type of documents to be validated (e.g. ID card, passport, driving licence).

8.4 Contra indicators

Age assurance systems can include multiple age assurance components and may have multiple sources of information from both primary and secondary credentials. These can lead to mismatches of data or information indicating that the claimed age is possibly not the true age.

These are called contra indicators.

When presented with a contra indicator, age assurance providers should (but are not limited to):

a) take action to resolve the contra indicator by gathering more evidence to verify if the age-related eligibility decision can be met, or

b) communicate the existence of the contra indicator to each relying party.

8.5 Fail safe

An age assurance system shall be fail safe.

This means that an age assurance result should not cause a relying party to make an incorrect age-related eligibility decision because of a system failure. This is a different issue to an age assurance result being a false positive or a false negative – that is addressed in performance characteristics (see Clause 6).

Age assurance systems should be designed with robust fail-safe mechanisms to ensure that, in the event of a system failure or malfunction, identity information cannot leak from the system and the default age-related eligibility decision shall be to deny access to the age restricted goods, content, service, venue or space.

The following characteristics outline how age assurance systems should fail safely.

a) In the event of a failure of a component of the system, that component should immediately cease the collection, processing and transmission of user data.

b) In the event of a data acquisition failure, the age assurance system should not establish an age assurance result.

c) In the event of a compromise to the connection between the age assurance system and the relying party, the system should not establish an age assurance result.

d) An age assurance system should revert to the safest default settings during a failure, ensuring that no additional personal information is inadvertently exposed or collected.

e) An age assurance system failure should be logged and subject to swift diagnosis and remediation, which can include a repetition of the age assurance process.

9 Acceptability characteristics

9.1 General

Age assurance systems should be designed and implemented to ensure inclusivity, providing equitable access and accurate results for all users, regardless of their demographic characteristics and cultural sensitivity.

This includes supporting multiple languages in which the age assurance system is intended to be used.

9.2 Inclusivity

Examples of approaches that can support inclusivity include:

a) using universal design principles, ensuring that it is accessible to individuals with diverse abilities, including those with disabilities;

b) conformity with standards such as the Web Content Accessibility Guidelines (WCAG);[18]

c) supporting multiple languages to accommodate users from different linguistic backgrounds; interfaces, instructions and support services should be available in the predominant languages of the contexts in which the age assurance system is intended to be used;

d) providing alternative input methods (e.g. voice commands, screen readers) to ensure that users who cannot use traditional input devices can still complete the age assurance process;

e) providing alternative age assurance methods;

f) ensuring that the system's design and implementation is culturally appropriate and sensitive to the norms and values of different user groups; this includes the use of culturally relevant imagery, language and examples; and

g) ensuring that age analysis is tested and validated across diverse demographic groups to prevent bias and ensure fair treatment of all users.

9.3 User engagement and assistance

Relying parties, supported by age assurance providers, should provide educational resources to help users understand the age assurance system, their rights and how their data will be protected. These resources should be accessible and understandable to all users.

Relying parties, supported by age assurance providers, should plan for and accommodate users with additional needs. These can include:

a) Users with disabilities – the visually impaired can require screen readers, magnification tools or Braille displays to interact with the system; the hearing-impaired can require visual alerts or captions for any audio prompts.

b) Individuals with limited hand dexterity or mobility can require alternative input methods, such as voice commands, adaptive keyboards or switch devices.

c) Older users – older adults experiencing cognitive decline can require simplified interfaces, clear instructions and additional time to complete tasks; it is possible that they are not familiar with modern technology and require more intuitive design and step-by-step guidance.

d) Children and adolescents – younger users can require systems that facilitate parental (or responsible adult) support, consent or supervision and they can require an interface and instructions that are age-appropriate and engaging for younger users.

e) Language barriers – users who do not speak the system’s primary language fluently can require multi-language support, including translations of the interface, instructions and support materials.

f) Low literacy users – individuals with low literacy levels can require instructions and prompts written in simple, clear language or the use of icons, images and diagrams to help convey information.

g) Access to technology – individuals who cannot afford personal devices or reliable internet access can require the age assurance system to be accessible through public access points, such as libraries or community facilities.

h) Limited internet access – users with limited or intermittent internet connectivity can require offline capabilities or low-bandwidth solutions, so it should be ensured that the system is usable in areas with limited infrastructure and technological resources.

i) Documentation issue – individuals who do not have standard forms of identification or consistent access to personal documents can require alternative age assurance methods.

Personnel involved in the development, implementation and support of the age assurance system should receive training on inclusivity principles and practices to ensure they are equipped to address the needs of diverse users.

9.4 Complaint handling

Relying parties shall provide means for individuals to register a complaint, including taking responsibility for any interaction with the age assurance provider on behalf of the user or individual.

Age assurance providers and relying parties shall enter into written agreement on which entity is responsible for complaint handling.

The user interface should provide a user-friendly and easily accessible mechanism for individuals to file complaints or report issues related to the age assurance system. This should include clear, age-appropriate instructions on how to lodge a complaint, including what information is needed and the steps involved in the process.

Relying parties should acknowledge receipt of complaints promptly, informing the individual that their issue is being reviewed and should establish and communicate a reasonable time frame within which complaints will be addressed and resolved.

Relying parties should ensure individuals can track the status of their complaint throughout the resolution process.

Age assurance providers and relying parties should generate regular reports on complaint outcomes to identify trends, improve processes, enhance system reliability and use these insights to continuously improve the age assurance system and address recurring issues.

10 Practice statements

10.1 General

Practice statements should document the practices, procedures and controls employed by an entity to fulfil its service. It should also include a description of how their system and practice statement are kept under continuous and regular review, including by the top management of the entity.

An age assurance provider should provide indicators of effectiveness and document the operational practices and procedures utilized to provide age assurance results.

A relying party should document the approaches to age assurance that it uses to ensure that its age-related eligibility decisions comply with relevant age-related eligibility requirements.

An intermediary that has a direct and independent impact on the achievement of the characteristics described in this document should prepare their own practice statement.

Each entity requiring an age-related eligibility decision and each entity contributing to its age assurance system should indicate whether the providers in its supply chain also have compatible practice statements.

An informative summary of practice statements should be made publicly available by the relevant entity. Though parts of the practice statement should be communicated to the public, other parts should only be communicated to auditors.

Practice statements communicated to the public should not contain information about the approaches used to detect and prevent attack vectors (see 8.3.2).

10.2 Practice statements by age assurance providers

A practice statement by an age assurance provider 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 requirement), including identifying any policy maker(s) who has established age-related eligibility requirements and the content of those requirements and acknowledgement of any intermediaries involved in the process;

b) a description of age assurance components utilized by the age assurance system, including:

   1) identifying the sources (including whether they are an authoritative source),

   2) identifying whether they rely on primary or secondary credentials,

   3) if used, identifying the age verification methods being deployed to establish an age assurance result,

   4) if used, identifying the age estimation methods being deployed to establish an age assurance result,

   5) if used, identifying the age inference methods being deployed to establish an age assurance result;

c) a description of the indicators of effectiveness achieved by the age assurance system;

d) a description of how the system undertakes the binding of the age assurance result to the correct individual;

e) a description of how the system can prevent collaborative attacks between individuals;

f) a description of how the age assurance provider approaches the protection of the privacy of users, including the data protection laws and obligations, which should include:

   1) how the age assurance system meets the privacy characteristics set out in this document and which privacy characteristics it supports,

   2) how only the minimal amount of personally identifiable information is processed for the purpose of meeting legal obligations and gaining the required indicators of effectiveness for age assurance to be established,

   3) how personally identifiable information gathered for the purpose of age assurance is limited to that purpose and stored (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable),

   4) how the age assurance provider will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made based on inaccurate or incomplete data, solely automated decisions and addressing breaches in the security of that data,

g) a description of how the age assurance methods adopted by the age assurance provider offer functionality appropriate to the capacity and age of a child or adult who can use the service;

h) a description of how the age assurance system addresses the security characteristics set out in this document and of which security characteristics are supported;

i) a description of how the age assurance provider secures that the use of the age assurance system is implemented in a manner that includes:

   1) approaches that are accessible and inclusive to users,

2) approaches that do not unduly restrict access of children or adults to services to which they should reasonably have access, e.g. news, health and education services,

3) 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.

j) a description of how the system, practice statement and approaches to the age assurance system are subject to audit, certification and review. In the case of an audit having taken place, there should be a description that includes:

1) the date when the audit was performed,

2) the name and qualifications of the auditor,

3) the major result(s) of the audit report.

10.3 Practice statements by relying parties

A practice statement by a relying party shall contain, as a minimum:

a) the criteria for age-related eligibility decisions (e.g. whether the eligibility is for individuals under, over or within a specified age range);

b) a description of age assurance providers (if any) utilized in the age assurance system, with appropriate cross-referencing to their practice statements, as well as acknowledgement of any intermediaries involved in the process;

c) a description of where the age-related eligibility requirements came from; in particular, identifying both the policy makers and the associated regulations or recommendations;

d) a description of the methods used by or on behalf of the relying party to establish an age assurance result including:

1) if used, identifying the age verification methods being deployed to establish an age assurance result, including the issuers relied upon, e.g. identity providers, digital credential issuers or both,

2) if used, identifying the age estimation methods being deployed to establish an age assurance result, including the age assurance intermediaries relied upon,

3) if used, identifying the age inference methods being deployed to establish an age assurance result, including the issuers relied upon, for example either identity providers or digital credential issuers or both,

4) if a result of an age assurance method is indeterminate or unknown, indicating which fall-back mechanism(s), method(s) or technique(s), if any, will be used, and

5) if applied, a description of configuration settings utilized and how they have impacted upon the requirements of this document;

e) a description of how the relying party approaches the protection of the privacy of users, including the data protection laws and obligations, which should include:

1) how the relying party minimizes the amount of personally identifiable information it collects and stores about individuals during making age-related eligibility decisions,

2) how personally identifiable information gathered for the purpose of age assurance is limited to that purpose and stored (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable),

3) how the relying party will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made based on inaccurate or incomplete data, solely automated decisions and addressing breaches in the security of that data,

4) how the personal data are secured, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures,

5) how the relying party and any intermediaries it uses, if any, meet(s) the privacy characteristics from Clause 7 of this document,

6) how the relying party and any intermediaries it uses, if any, meet(s) the security characteristics from Clause 8 of this document, and

7) how the relying party and the age assurance method(s) that it uses, if any, meet(s) the acceptability characteristics from Clause 9 of this document;

f) a description of how the age assurance methods adopted by the relying party offer functionality appropriate to the capacity and age of a child or adult who can use the service,

g) a description of how the relying party that secures the use of the age assurance system is implemented in a manner that includes:

1) approaches that are accessible and inclusive to users with protected characteristics or additional needs,

2) 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,

3) 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 an individual can seek redress;

i) a description of how the system, practice statement and approaches to age assurance are subject to audit, certification and review.

10.4 Practice statements by intermediaries

A practice statement by an intermediary shall contain, as a minimum:

a) a description of the role played by the intermediary and how they have a direct and independent impact on the achievement of the characteristics of age assurance systems specified in this document;

b) a description of age assurance providers or relying parties that the intermediary supports, with appropriate cross-referencing to their practice statements;

c) a description of how the intermediaries' activity, system, practice statement and approaches to age assurance is subject to audit, certification and review.

Bibliography

[1] ISO 8601(all parts), *Date and time — Representations for information interchange*

[2] ISO 10007:2017, *Quality management — Guidelines for configuration management*

[3] ISO/IEC/TR 10032:2003, *Information technology — Reference Model of Data Management*

[4] ISO/IEC 13888-1:2020, *Information security — Non-repudiation — Part 1: General*

[5] ISO/IEC/TS 19249:2017, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications*

[6] ISO/IEC 19794-1, *Information technology — Biometric data interchange formats — Part 1: Framework*

[7] ISO/IEC 24760-1:2025, *Information security, cybersecurity and privacy protection — A framework for identity management — Part 1: Core concepts and terminology*

[8] ISO/IEC 25010:2023, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model*

[9] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[10] ISO/TR 27877:2021, *Statistical analysis for evaluating the precision of binary measurement methods and their results*

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

[12] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

[13] ISO/IEC 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*

[14] ISO 29995:2021, *Education and learning services — Vocabulary*

[15] ISO/IEC 30107-1:2023, *Information technology — Biometric presentation attack detection — Part 1: Framework*

[16] ISO 31700-1:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*

[17] ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

[18] W3C Web Content Accessibility Guidelines (WCAG) 2.2, 5 October 2023; updated 12 December 2024

ICS 35.030
Price based on 29 pages

iso.org