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)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
3.1 Terms relating to age assurance 1
3.2 Terms relating to actors and parties 3
3.3 Terms relating to data and processes 4
4 Overview of age assurance **7**
4.1 Age 7
4.2 Characteristics of age assurance systems 7
4.3 Age assurance methods 8
4.3.1 Overview of age assurance methods 8
4.3.2 Age verification methods 8
4.3.3 Age estimation methods 9
4.3.4 Age inference methods 10
4.3.5 Successive validation 10
4.4 Stakeholders 10
4.4.1 General 10
4.4.2 Policy makers 10
4.4.3 Consumer protection agencies 11
4.4.4 Sector associations 11
5 Functional characteristics **11**
5.1 Age assurance systems 11
5.1.1 General 11
5.1.2 Age assurance providers 11
5.1.3 Intermediaries 12
5.2 Data acquisition for age assurance components 12
5.2.1 Sources of data 12
5.2.2 Primary and secondary credentials 12
5.2.3 Date transposition errors 13
5.3 Binding of age assurance result to the correct individual 13
5.3.1 Binding characteristics 13
5.3.2 Approaches to binding 13
5.4 Age assurance data processing 14
5.5 Configuration management 14
5.6 Context in use 15
5.7 Delivery of age assurance result 15
6 Performance characteristics **15**
6.1 Performance effectiveness 15
6.1.1 General 15
6.1.2 Effective age assurance systems 15
6.1.3 Ineffective age assurance systems 16
6.1.4 Use of self-asserted age 16
6.1.5 Other factors affecting effectiveness 16
6.2 Indicators of effectiveness 16
6.3 Performance metrics 17
6.3.1 Classification accuracy 17
6.3.2 Primary metrics 17
6.3.3 Outcome error parity 17
6.3.4 Performance efficiency 17
6.4 Resource utilization 18
6.5 Testability 18

© ISO/IEC 2025 – All rights reserved

7 Privacy characteristics **18**
7.1 General 18
7.2 Privacy by design and default 18
7.3 Data minimization 19
7.3.1 Collection limitation 19
7.3.2 Non-disclosure of age-related data 19
7.3.3 Compliance with legal obligations 19
7.3.4 Purpose limitation 19
7.3.5 Access control 19
7.3.6 Data disposal 19
7.4 Avoidance of adding to digital footprint 19
7.5 User awareness 20
7.6 Audit logs 20

8 Security characteristics **21**
8.1 Security by design and default 21
8.2 Replay, forwarding or reuse of age assurance result 21
8.2.1 Replay of an age assurance result 21
8.2.2 Forwarding of an age assurance result 21
8.2.3 Planned memorization or reuse of an age assurance result 21
8.3 Resistance to attack 22
8.3.1 Preparation for attack 22
8.3.2 Attack vectors 22
8.3.3 Biometric presentation attacks 22
8.3.4 Spoofing attack 23
8.3.5 Counterfeiting attack 23
8.4 Contra indicators 23
8.5 Fail safe 23

9 Acceptability characteristics **24**
9.1 General 24
9.2 Inclusivity 24
9.3 User engagement and assistance 24
9.4 Complaint handling 25

10 Practice statements **25**
10.1 General 25
10.2 Practice statements by age assurance providers 26
10.3 Practice statements by relying parties 27
10.4 Practice statements by intermediaries 28

Bibliography **29**

© ISO/IEC 2025 – All rights reserved

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.

© ISO/IEC 2025 – All rights reserved

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.

© ISO/IEC 2025 – All rights reserved

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.]

© ISO/IEC 2025 – All rights reserved

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

© ISO/IEC 2025 – All rights reserved

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.

© ISO/IEC 2025 – All rights reserved

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

© ISO/IEC 2025 – All rights reserved

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]

© ISO/IEC 2025 – All rights reserved

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)

© ISO/IEC 2025 – All rights reserved

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.

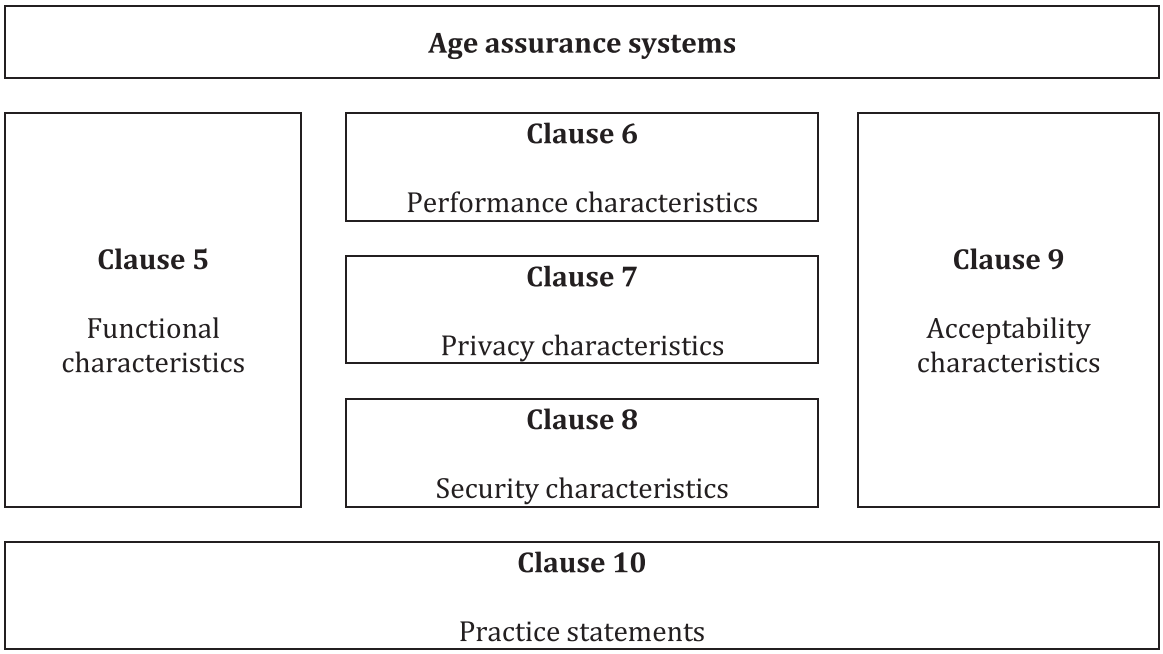


Figure 1 — Structure of the framework of age assurance systems

© ISO/IEC 2025 – All rights reserved