



BSI Standards Publication

Information security, cybersecurity and privacy protection — Age assurance systems

Part 1: Framework

National foreword

This British Standard is the UK implementation of ISO/IEC 27566-1:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5/5, Age Assurance Standards.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 30438 1

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2025.

Amendments/corrigenda issued since publication

Date	Text affected
<hr/>	



International
Standard

ISO/IEC 27566-1

**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

**First edition
2025-12**

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

Full document details: BS ISO/IEC 27566-1:2025

© ISO/IEC 2025



Documents

Document Sharing Hub



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

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

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