



DPC: 25/30486825 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 20 December 2024

Origin: International

Latest date for receipt of comments: 12 February 2025

Project No. 2024/00297

Responsible committee: IST/33/5 Identity Management and Privacy Technologies

Interested committees:

Title: Draft BS EN ISO/IEC 27566-1 BS EN ISO/IEC 27566-1 Information security, cybersecurity and privacy protection — Age assurance systems — Framework. Part 1: Framework.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 12 February 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27566-1

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

Part 1: Framework

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-12-20

Voting terminates on:
2025-03-14

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27566-1:2024(en)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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 Age assurance terms	1
3.2 Actors and parties	3
3.3 Data and processes	4
4 Abbreviations	6
5 Overview of age assurance	6
5.1 Age	6
5.2 Characteristics of age assurance systems	7
5.3 Age assurance methods	8
5.3.1 Overview of age assurance methods	8
5.3.2 Age verification methods	8
5.3.3 Age estimation methods	9
5.3.4 Age inference methods	9
5.3.5 Successive validation	10
5.4 Stakeholders	10
5.4.1 Policy makers	10
5.4.2 Consumer protection agencies	11
5.4.3 Sector associations	11
6 Functional characteristics	11
6.1 Age assurance systems	11
6.1.1 General	11
6.1.2 Age assurance providers	12
6.1.3 Intermediaries	13
6.2 Data acquisition for age assurance components	13
6.2.1 Sources of data	13
6.2.2 Primary and secondary credentials	13
6.2.3 Date transposition errors	14
6.3 Binding of age assurance result to the correct individual	14
6.3.1 Binding characteristics	14
6.3.2 Approaches to binding	14
6.4 Age assurance data processing	15
6.5 Configuration management	15
6.6 Context in use	15
7 Performance characteristics	16
7.1 General	16
7.1.1 Effective age assurance systems	17
7.1.2 Ineffective age assurance systems	17
7.1.3 Use of self-asserted age	17
7.1.4 Other factors affecting effectiveness	17
7.2 Indicators of confidence	18
7.3 Performance metrics	18
7.3.1 Classification Accuracy	18
7.3.2 Primary metrics	18
7.3.3 Outcome error parity	19
7.3.4 Performance efficiency	19
7.4 Resource utilisation	19
7.5 Testability	19
8 Privacy characteristics	19

8.1	General.....	19
8.2	Privacy by design and default.....	20
8.3	Data minimization.....	21
8.3.1	Collection limitation.....	21
8.3.2	Non-disclosure of age-related data.....	21
8.3.3	Compliance with legal obligations.....	21
8.3.4	Purpose limitation.....	21
8.3.5	Access control.....	21
8.3.6	Data disposal.....	21
8.4	Avoidance of adding to digital footprint.....	21
8.5	User awareness.....	22
8.6	Audit Logs.....	22
9	Security characteristics.....	23
9.1	General.....	23
9.2	Security by design and default.....	23
9.3	Freshness, Reuse and Forwarding of age assurance result.....	24
9.3.1	Freshness of an age assurance result.....	24
9.3.2	Forwarding of an age assurance result.....	24
9.3.3	Planned memorization or reuse of an age assurance result.....	24
9.4	Resistance to presentation attack.....	24
9.4.1	Preparation for attack.....	24
9.4.2	Attack vectors.....	25
9.4.3	Biometric presentation attacks.....	25
9.4.4	Spoofing attack.....	25
9.5	Contraindicators.....	25
9.6	Fail safe.....	26
10	Acceptability characteristics.....	26
10.1	General.....	26
10.2	Inclusivity.....	27
10.3	User engagement and assistance.....	28
10.4	Complaint handling.....	28
11	Practice statements.....	29
11.1	General.....	29
11.2	Practice statements by age assurance providers.....	30
11.3	Practice statements by relying parties.....	31
11.4	Practice statements by intermediaries.....	32
	Bibliography.....	33

Foreword

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

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

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

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

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

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

This is a first edition.

A list of all parts in the ISO 27566 series can be found on the ISO website.

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

Introduction

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

Age-related eligibility decisions are required when a person should 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 to be provided.

This document aims to solve the problem of 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 may in some instances be connected to identity verification but can also be performed in ways other than via identity verification.

The aim of this document is to enable policy makers (like government, regulators or providers of age restricted goods, content, services, venues or spaces) to specify applicable types of age assurance systems and associated indicators of confidence 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 some 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 control,
- 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 need to be presented vary widely among different countries or even between different states within a federated country.

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

Part 1: Framework

1 Scope

This document establishes core principles, including privacy and security, for the purpose of 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 terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 Age assurance terms

3.1.1

age assurance

set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make *age-related eligibility decisions* (3.1.8) 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, over or under a certain age or within an age range

3.1.3

identity

set of attributes related to an entity

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2]

3.1.4

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).

3.1.5

evidence

information supporting the occurrence of an event or action

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

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

3.1.6

age-related eligibility

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

3.1.7

age-related eligibility requirement

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

3.1.8

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

3.1.9

age verification method

age assurance method 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) may be applicable.

3.1.10

age estimation method

age assurance method based on analysis of biological or behavioural features of humans that vary with age

3.1.11

age inference method

age assurance method 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

3.1.12

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](#))

3.1.13

practice statement

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

3.1.14

indicators of confidence

quantitative, qualitative or descriptive measures that demonstrate how well an *age assurance system* ([3.3.3](#)) meets functional, performance, privacy, security and acceptability characteristics

3.1.15

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 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](#))

3.2.2

relying party

entity that relies on an *age assurance result* ([3.1.2](#)) to make an *age-related eligibility decision* ([3.1.8](#))

3.2.3

intermediary

entity that facilitates the interaction between individuals, *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](#))

Note 1 to entry: Examples of an intermediary include credit agencies, mobile network operators or orchestration service providers.

3.2.4

policy maker

entity responsible for establishing *age-related eligibility requirements* ([3.1.7](#)) for access to goods, content, services, venues or spaces

EXAMPLE a policy maker can be governmental, regulatory, an authorising organization, enterprise, relying party or person.

Note 1 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* ([3.1.8](#))

Note 1 to entry: An age-related eligibility decision maker could 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 is recognized to have the right to create and manage a record that contains a set of attributes that allows an *individual* ([3.2.9](#)) to be uniquely identified within a given context

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 may be the same entity.

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

3.3 Data and processes

3.3.1

age assurance component

part of an *age assurance system* ([3.3.3](#))

3.3.2

age assurance method

method 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 *age assurance methods* ([3.3.2](#)) to provide an *age assurance result* ([3.1.2](#))

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 the present 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**contraindicator**

information that calls into question or otherwise indicates that either an *age assurance result* (3.1.2) may not be correct or that the *binding* (3.3.18) of the age assurance result to the right *individual* (3.2.9) may not be correct or both.

Note 1 to entry: Contraindicators 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 *age assurance system* (3.3.3) with the goal of interfering with the operation of the system

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 or physiological functions or voluntary reactions or subject behaviours

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

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

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

[SOURCE: adapted from 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 that provides evidence of age associated with the *individual* (3.2.9)

Note 1 to entry: This document 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) containing an accurate representation of the age of the *individual* (3.2.9)