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.

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