ISO/IEC JTC 1/SC 27/WG 5 **N 3927**

ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies"
Convenorship: **DIN**
Convenor: **Rannenberg Kai Mr Prof. Dr.**

ISO/IEC AWI 27566-1

Document type	Related content	Document date	Expected action
Ballot / Reference document	Ballot: ISO/IEC AWI 27566-1 (restricted access)	2023-12-05	**COMMENT/REPLY** by 2024-01-30

ISO/IEC 27566-1:2025

ISO/IEC JTC1/SC27/WG5

Secretariat: DIN

Information security, cybersecurity and privacy protection – Age assurance systems – Part 1 – Framework

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes d'assurance de l'âge – Partie 1 – Cadre de travail

WD2.0

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

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.

To help you, this guide on writing standards was produced by the ISO/TMB and is available at https://www.iso.org/iso/how-to-write-standards.pdf

A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf

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

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 and/or on the ISO list of patent declarations received (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 ##### 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 principles 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 a natural person and the supplier of any product, content or service that has policy requirements for acquiring assurance about the age 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 or service to be provided.

This document aims to solve the problem of inadequately defined age assurance processes and associated lack of trust in terms of efficacy, acceptability, privacy and security. Age assurance systems implemented using this document are seeking to balance the privacy outcomes that will address needs of implementers, individuals and policy makers.

Although a natural person's age is an attribute of their identity, it is not necessarily the case that establishing the full identity of a natural person 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 age restricted product, content or service suppliers) to specify applicable types of age assurance systems and associated indicators of confidence in their particular policy requirements.

As an example, a policy maker may determine that, in order to authorise the sale of liquor, a decision maker shall use some specific type of age assurance systems to a specified indicator of confidence 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 are appropriate for each type of age-related eligibility decision – that is a matter for policy makers.

This document does not:

- Establish or hinder the establishment of any methodologies (called assurance components in this document) for age assurance systems but indicates that three types of age assurance techniques can be used: age verification, age estimation and age inference
- Establish or recommend the age assurance thresholds or determine the required indicators of confidence for different products, content or services – these are matters for policy makers
- Deal with financial or commercial models for age assurance systems – these are a matter for economic operators in the age assurance process
- Address, except for some specific objectives applicable to age assurance systems, the requirements for data protection – these are a matter for data controllers
- Establish requirements for interoperability, age assurance exchanges or communities of interest for age assurance systems – these could be a matter for future standards, technical specifications or technical reports

Information security, cybersecurity and privacy protection – Age assurance systems – Part 1 – Framework

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes d'assurance de l'âge – Partie 1 – Cadre de travail

1 Scope

This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about the age of, or an age range for, a natural person.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

— ISO/IEC 24760-1, *Information technology — Security techniques — A framework for identity management: Terminology and concepts*

— ISO/IEC 24760-2, *Information technology — Security techniques — A framework for identity management: Reference architecture and requirements*

— ISO/IEC 24760-3, *Information technology — Security techniques — A framework for identity management: Practice*

— ISO/IEC 27701, *Information technology – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

— ISO/IEC 29115, *Information technology – Security techniques – Entity authentication assurance framework*

— ISO/IEC 30107-1, *Information technology – Biometric presentation attack detection – Part 1:Framework*

Editor's Note:

If these references are not referred to in the text indicating a normative requirement, then they should be moved to the bibliography at the end.

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 http://www.electropedia.org/

Editor's Note:

At the 42nd Meeting of ISO/IEC JTC 1/SC 27/WG 5, Experts agreed that the definitions should be presented in semantic groupings, to aid global translation and ease of reference. Suggestions from contributors are invited as to which semantic groups may be appropriate and helpful.

3.1
age assurance
process of establishing, determining, and/or confirming an age assurance attribute

3.2
age assurance practice statement
statements of the procedures and the operational practices that an organization employs when providing a age assurance service

Note to entry: See clause 4.4

3.3
age assurance service provider
organization responsible for processes establishing or computing age attributes

3.4
age assurance service
service provided individually or collectively by age assurance service providers

Note to entry: An age assurance service can consist of one or more organisations

3.5
age assurance attribute
attribute indicating that a natural person is a certain age, over or under a certain age or within an age range

3.6
age estimation
age assurance attribute established using inherent features or behaviours related to a natural person

3.7
age-related eligibility
right of access to goods, content or services based on an age limit or an age band

3.8
age verification
age assurance attribute based on calculating the difference computation between the current date and the date of birth of a natural person

3.9
age inference
age assurance attribute based on the presence of information which indirectly implies that a natural person is over or under a certain age

3.10
artificial intelligence
branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement

[SOURCE: ISO/IEC 2382:2015, Information technology — Vocabulary]

3.11

attack vector

path or means by which one or more persons attempt to circumvent the age assurance process in order to obtain a malicious outcome

3.12

attribute

characteristic or property of an entity

[SOURCE: ISO/IEC 24760-1: 2019, 3.1.3]

Note to entry: within the context of this document, the entity is a natural person.

3.13

attribute server

server trusted by one or more natural persons and one or more age assurance service providers to issue attributes related to a natural person

3.14

authoritative party

entity that has the recognized right to create or record, and has responsibility to directly manage, an attribute associated with an individual

Note to entry: Jurisdiction(s) and/or industry communities sometimes nominate a party as authoritative. It is possible that such a party is subject to legal controls. See clause 4.1.2 for a more detailed explanation.

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

3.15

authoritative source

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

[SOURCE: ISO/IEC 29115:2013(en), 3.5]

3.16

client application

piece of software/hardware used by a user to interact with other remote components

3.17

community of interest

group of parties, members of a trust framework, who wish to obtain or verify an age assurance attribute relating to a natural person

NOTE Members of a community of interest can include relying parties and age assurance service providers.

3.18

contra-indicator

evidence or pieces of information that call into question or otherwise indicate that an age assurance attribute may not be correct

Note to entry: Contra-indicators can be at a natural person 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.

3.19

decision maker

organization or person responsible for making an age-related eligibility decision

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

3.20

evidence

information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

[SOURCE: ISO/IEC 13888-1: 2009, 3.11]

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

3.21

identifying attribute

attribute that contributes to uniquely identifying a natural person within a given context

[SOURCE: ISO/IEC 29003:2018, 3.8]

3.22

identity

set of attributes which makes it possible to identify a natural person within a given context

[SOURCE: ISO/IEC 29003:2018, 3.9]

3.23

identity information provider

entity that makes available identity information

Note 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 24760-1:2011, 3.3.4]

3.24

indicators of confidence

quantitative, qualitative or descriptive measure of the correctness and accuracy to which an age assurance attribute can be stated to relate to a natural person

Note to entry: Further information about indicators of confidence is in clause 6.

3.25

binding

property that relates an age attribute to the correct natural person

3.26

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: ISO/IEC 30107-1:2016, 3.2]

3.27

liveness detection

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

[Source: ISO/IEC 30107-1:2016, 3.3]

3.28

policy maker

governmental, regulatory, authorising organisation, corporation or person responsible for establishing age-related eligibility requirements for access to goods, content or services

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

3.29

presentation attack

presentation to the age assurance system with the goal of interfering with the operation of the system

Note to entry: For Biometric Presentation Attack Detection see ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework, however, this standard also refers to documentary or record presentation attacks

3.30

primary credential

document or record from an authoritative party that provides evidence of attributes associated with natural person

Note 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).

3.31

relying party

actor that relies on an age assurance assertion or claim to make an age-related eligibility decision

[SOURCE: ISO/IEC 29115:2013(en), 3.22 (adapted)]

3.32

relying party practice statement

statements of the procedures and the operational practices that a relying party employs to enable age-related eligibility decisions

3.33

secondary credential

an attribute relating to a natural person derived from one or more primary credentials

3.34

social proofing

analysis of the digital footprint and the related social graphs of a natural person

3.35

trust

degree to which a user or other stakeholder has confidence that a product or system will behave as intended

[SOURCE: ISO/IEC 25010:2011, 4.1.3.2]

3.36

unlinkability

property that ensures that a PII principal may make multiple uses of resources or services without others being able to link these uses together

[Source: ISO/IEC TR 27550:2019, 3.25]

3.37

untraceability

property that ensures that an age assurance attribute used by a natural person in a particular context cannot be traced to that natural person by a relying party

Note to entry: Untraceability applies to other third parties not being able to trace back to the age assurance service provider, but individuals would be aware of the age assurance service provider to be able to exercise their data rights.

4 Characterisation of age assurance systems

4.1 General

An Age Assurance System shall consist of:

(a) One or more assurance components, and

(b) An age processing sub-system.

[Recommendation to insert a diagram] – Please see suggestions at the end of this draft document

4.1.1 Age assurance components

Age assurance components indicate an attribute that determines natural person’s age. They are established by capturing information from or about a natural person regarding:

(a) Something that they know about themselves or about others (such as their date of birth)

(b) Something that they possess, which is usually only possessed by persons of a known minimum age (such as a credit card) or which includes the attribute of date of birth

(c) Something that they are or are inherent features about them (such as biometrics, behaviours or appearance)

(d) An attestation by a trusted third party (such as a parent or legal guardian)

Age assurance components establish age assurance attributes or may combine multiple sources together to elevate trust in the attributes associated with the natural person.

The assurance components can include:

(a) A claimed attribute by the person that expresses the age – known as a self-asserted age attribute
(b) A process or system deriving an attribute that expresses the age from an identity document from an authoritative source - for example an 18-plus assurance attribute derived from the date of birth in a passport
(c) A process or system deriving an attribute that expresses the age from primary or secondary credentials, a data set, another age assurance service provider or identity information provider
(d) A process or system deploying artificial intelligence to derive probable age from one or more biometric identifiers, behaviours, characteristics or actions of individuals
(e) A process or system deploying social proofing to obtain or verify age assurance attributes
(f) A process or system deriving an inference of age assurance attributes from the presence of characteristics, features or possessions of a natural person
(g) A process or system based on the attestation of trusted parties (such as parents or legal guardians) or an authoritative source (such as governments, schools or employers) about the age of a person
(h) An assessment led by a trained person in the process assessing elements that take into account a person's appearance, demeanour, background and credibility in person or online
(i) A process or system that derives age assurance attributes from any other method that can establish indicators of confidence

[Recommendation to insert a diagram] – Please see suggestions at the end of this draft document

4.1.2 Primary and secondary credentials

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

A primary credential is a document or record issued by an authoritative party used by a natural person to provide evidence for some set of attributes. The authoritative party is an entity that has the recognized right to create a document or record and has responsibility to directly manage an identifying attribute. It could be a governmental agency, public body or a private body established for such purposes.

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

A secondary credential is an attribute relating to a natural person derived from a primary credential. It may be 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. As an example, a bank may establish an account record from an authentication process involving capturing data from a natural person'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 natural person, is the creation of a secondary credential.

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

4.1.3 Age assurance processing sub-system

An age assurance processing sub-system may include a process or system for:

(a) gathering together assurance components from multiple sources
(b) identifying attack vectors, protecting against presentation attack and assessing the liveness of individuals
(c) identifying and addressing contraindicators
(d) elevating the trust in an age attribute through multiple sources
(e) individuals to exercise data rights
(f) dissemination of age attributes, to a indicators of confidence, to relying parties
(g) monitoring, continuously improving and learning from age assurance activities
(h) one or more sources of age assurance components
(i) monitoring and logging the activities and outputs of the sub-system
(j) providing transparency reporting to authorized entities (e.g., regulators, auditors, certification bodies and researchers)
(k) developing and publishing age assurance practice statements in appropriate human readable and machine readable formats

[Recommendation to insert a diagram] – Please see suggestions at the end of this draft document

4.2 Guidance for policy makers

A policy maker can determine:

(a) the age-related eligibility requirements for access to some goods, content or services;

(b) the permitted age assurance solutions;

(c) the criteria to be met by the age assurance service providers and any special provisions relating to the handling, storage and security of age and identifying attributes by age assurance service providers; and

(d) the appropriate entity authentication factors to be used by age assurance service providers.

A policy maker may be internal to a relying party or an external body (governmental, regulatory or authorising organisation).

Where a policy maker is external to the relying party, they can implement the policy through legislative or non-legislative means, through permissions, authorisations or licensing requirements or through guidance or policy documents. An external policy maker should consult relevant stakeholders and decision makers before establishing a policy and regularly review the policies to take account of societal and technological change.

A policy maker may remain neutral to technological approaches or approve and regularly review certain particular technological approaches. A policy maker may also opt to specify approaches which are unsuitable, for instance deemed too easy to circumvent.

4.3 Categorisation of age assurance solutions

4.3.1 Age verification

Age verification can involve the use of a document bearing the date of birth of the natural person or authoritative sources of data about the natural person, where the age is computed using the time difference between the current date and the date of birth of the natural person without necessarily revealing the date of birth of the natural person to the supplier of the goods, content or services.

Guidance: If such verification were done directly by the supplier of goods, content or services, it would necessarily acquire more information than strictly needed. The use of an age assurance service provider allows that concern to be addressed.

4.3.2 Age estimation

Age estimation involves the use of techniques where age assurance attributes are estimated using inherent features or behaviours related to a natural person.

Such techniques can use the biometric characteristics of the natural person (e.g. face and/or voice) or information derived from their social behaviour (e.g. using social media data).

Examples: Face analysis (e.g. using a short video) or voice analysis can involve the use of artificial intelligence systems.

The presentation of a biometric spoof (e.g. a facial image or video of a person on a tablet or a fake silicone or gelatine fingerprint) to a biometric sensor can be detected by methods broadly referred to as presentation attack detection, PAD. ISO/IEC 30107-1 establishes a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed and communicated for subsequent decision making.

The analysis of social media data can also involve the use of artificial intelligence systems, but can simply involve the use of more classic algorithms such as keyword detection.

4.3.3 Age inference

Age inference involves the use of techniques where one or more age assurance attributes can be inferred from the validity of a credential that provides information that allows the age of the natural person to be implied.

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 attribute to be established that the named individuals are "over 16" or have been emancipated to the age of 16.

Example 2: If an attestation of trusted parties (such as parents or legal guardians) of a minor is produced and can be verified, then an age assurance attribute for that minor can be derived from that attestation.

4.4 Age assurance practice statements

4.4.1 General

An age assurance service provider shall document the operational practices and procedures utilised to provide assured age attributes.

A relying party shall document the acceptable approaches to age assurance that it adopts to comply with age-related eligibility decisions that it takes. See Annex A for informative guiding principles that may assist a relying party (including a policy maker internal to a relying party) in the development of their relying party practice statement.

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

4.4.2 Content of age assurance practice statements

An age assurance practice statement 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 requirements)

(b) A description of age assurance components utilised by the age assurance system, including:
  a. identifying the attribute sources (including whether or not they are an authoritative source);
  b. identifying whether or not they rely on primary or secondary credentials;
  c. if used, identifying the age verification systems being deployed to establish an age assurance attribute
  d. if used, identifying the age estimation systems being deployed to establish an age assurance attribute
  e. if used, identifying the age inference systems being deployed to establish an age assurance attribute

(c) A description of the indicators of confidence necessary from the system or process in accordance with the vocabulary of this document

(d) A description of how the system performs user authentication using ISO/IEC 29115 framework

(e) A description of how the age assurance service provider approaches protecting the privacy of users, including the data protection laws and obligations, which shall include:
  a. how the age assurance system meets the privacy objectives in clause 7 of this document
  b. how only the minimal amount of personally identifiable information is processed for the purpose of gaining the required indicators of confidence for age assurance to be established;
  c. how personally identifiable information gathered for the purpose of age assurance is limited to that purpose (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable);
  d. how the party will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made on the basis of inaccurate or incomplete data, solely automated decisions and addressing breaches in the security of that data

(f) A description of how the age assurance approaches offer functionality appropriate to the capacity and age of a child or adult who might use the service;

(g) A description of how the age assurance system addresses the security objectives in clause 8 of this document;

(h) A description of how the age assurance provider secures the use of the age assurance system is implemented in a manner that includes:
  a. approaches that are accessible and inclusive to users with protected characteristics or additional needs
  b. 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;
  c. 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

(i) A description of how the system, practice statement and approaches to age assurance system is subject to annual review, including by the age assurance service provider or relying party.

4.5 Age assurance service providers

An age assurance service provider may be placed between an individual and a relying party. It avoids the unnecessary direct sharing of potentially personal data between the natural person and the relying party. Its role is to check some characteristics of an individual in order to derive some attributes from these characteristics without communicating all these characteristics to the relying party.

When a single age assurance service provider is placed between a natural person and a relying party, its main role is to preserve the privacy of the individual towards the relying party by disclosing the minimum set of personal information and should provide no more information than the relying party already knew about the individual, if any.

A single age assurance service provider can support an age verification process, an age estimation process or an age inference process or a combination of these.

An age assurance service provider may require its users to authenticate before being able to provide its service. This is the case in particular when they are providing an age verification process, since the date of birth of the individual must be reliably known to the age assurance service provider.

In such a case, an age assurance service provider shall use a document or a record about the individual issued by an authoritative party. The authoritative party is an entity that has the recognized right to create or record, and has responsibility to directly manage, attributes associated with an individual. It can be a governmental agency, a public body or a private body established for such purposes.

Care should be taken by the age assurance service provider to make sure that the attributes have not been issued inappropriately, to the wrong individual, with incorrect data on it, or may have been subject to falsification (e.g. if using a fake driving licence, a doctored passport or a falsified record in a database).

4.6 Acceptability of age assurance systems from the point of view of the individual

An individual shall be able to make their own opinion whether the solution fulfils the set of criteria that they believe to be necessary either from a privacy point of view or from a security point of view.

In order to help individuals to make their own opinion, each solution shall publicly disclose how/if the privacy objectives (see clause 6) are met and how/if the security objectives (see clause 7) are met in their age assurance practice statement.

5 Age assurance attribute

In this document, age is expressed as a real number that is expressed in the time that has passed since the subject’s birthday on the day in question.

A relying party may need to obtain an age assurance attribute before the delivery of goods, content or services. Within the class of age assurance attributes, four types of age assurance attributes may be requested by a relying party:

(a) the actual age,
(b) over a certain age,
(c) under a certain age, or
(d) within an age range.

Examples: "> 16", "< 60" and "18 < x > 30".

The first three types of age assurance attributes can be modelled as a single-valued attribute while the fourth type can be modelled as a multi-valued attribute, where the first value indicates under which age the natural person should be and the second value indicates over which age the natural person should be.

A person being “under a certain age” and “within an age range” has time-limited validity, which should be taken into account when considering the deployment of age assurance systems.

6 Indicators of confidence in age assurance

6.1 General

The indicators of confidence associated with an age assurance attribute can be determined by the process deployed to ensure that the age attribute relating to the natural person in question is correct.

The indicators of confidence can be used by policy makers to set an age assurance policy (see clause 4.2).

This standard establishes five core indicators of confidence:

(a) Asserted age assurance
(b) Basic age assurance
(c) Standard age assurance
(d) Enhanced age assurance
(e) Strict age assurance

The approaches to measurement and testing of age assurance could be structured around these indicators of confidence.

However, policy makers, relying parties and age assurance service providers may identify a need to sub-divide these indicators of confidence to provide greater granularity for a particular use case. Additionally, policy makers, relying parties and age assurance service providers may determine that age assurance attributes with some indicators of confidence either can not or could not be applicable to a particular age-related eligibility decision.

Further guidance about indicators of confidence is provided in Annex B (informative).

This document does not establish the specific characteristics of the five core indicators of confidence, but in general they can be described as follows:

6.1.1 Asserted age assurance

Asserted age assurance is the age claimed by the natural person by self-declaration or without the application of age assurance components. An asserted age can be captured in a data capture process, by reference to questions asked of the natural person or by historical assertion of age.

No attempt is made to validate the claimed age attribute.

An asserted age provides a low indicator of confidence that the age is assured to be the true age. An asserted age is not necessarily an incorrect age.

Asserted age assurance has validity at the time the attribute was claimed for a purpose where a low indicator of confidence is acceptable, but it has little value as a source of age assurance for future purposes. However, a change in a claimed age attribute by the same person may be a contra-indicator.

Note to entry: In most cases, an asserted age is unlikely, by itself, to provide sufficient age assurance for regulated age-related eligibility decisions, but may be satisfactory for simple, low risk, user experience workflows in applications (such as where the user is merely being asked in what level of detail they would like information to be presented to them). The indicators of confidence can be increased marginally through technical measures, such as preventing repeat attempts at entering a date of birth or age, or not guiding the client by preventing the entry of an age which would make them ineligible.

6.1.2 Basic age assurance

Basic age assurance is the age claimed by the natural person by self-declaration with the application of at least one age additional assurance component.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of an age assurance component process.

The age assurance component process may include for the simple validation of the claimed age attribute.

A basic age assurance may still leave unresolved contra indicators – see s.8.6, which should be communicated to the relying party.

The overall accuracy of basic age assurance would tend to show that the output is correct 9 times out of 10.

6.1.3 Standard age assurance

Standard age assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least one age assurance component to validate the claimed age by reference to attributes related to the natural person.

Unless stated otherwise in an age-related eligibility policy, standard age assurance shall be the age-related eligibility policy by default.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of an age assurance component process.

The age assurance component process shall include for the validation of the claimed age attribute.

The process shall include mechanisms to deter false or inaccurate self-declarations being made. An attempt shall be made to reduce the attack vector from bots or automated processes and to prevent false or inaccurate self-declarations being made.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

The overall accuracy of standard age assurance would tend to show that the output is correct 99 times out of 100.

6.1.4 Enhanced age assurance

Enhanced age assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least two other age assurance components from two independent sources (one of which shall be a primary or secondary credential) to validate the claimed age by reference to attributes related to the natural person.

The age assertion can be captured in a data capture process, by reference to questions asked of the natural person, by historical assertion of age or by inviting the user to submit evidence in support of the age assurance component processes.

The age assurance component processes shall include for the validation of the claimed age attribute.

An age assurance system providing enhanced age assurance should not be susceptible to attack vectors from bots or automated processes and should prevent false or inaccurate self-declarations being made.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

The overall accuracy of enhanced age assurance would tend to show that the output is correct 999 times out of 1000.

Note to entry: Enhanced age assurance is likely to be useful for policy makers considering higher risk goods, content or services; where there may be a significant risk to the health, safety or wellbeing of individuals.

6.1.5 Strict age assurance

Strict age assurance is the age claimed by the natural person by implied or actual self-declaration taken together with at least two other age assurance components from two independent sources (one of which shall be a primary credential) to validate the claimed age by reference to attributes related to the natural person.

The age assertion can be captured in a data capture process by inviting the user to submit evidence in support of the age assurance component processes.

The age assurance component processes shall include for the validation of the claimed age attribute.

All contra indicators identified shall be resolved or communicated to the relying party – see s.8.6.

The overall accuracy of strict age assurance would tend to show that the output is correct 9999 times out of 10000.

Strict age assurance should repeated at each age-related eligibility decision, by repeating the age assurance process.

Note to entry: Strict age assurance is likely to be useful for policy makers considering very high risk goods, content or services; or where seeking to safeguard the health, safety or wellbeing of individuals engaged in making or using very high risk goods, content or services.

6.2 Use of indicators of confidence

Depending upon the underlying technique(s) being used, age assurance service providers may not be able to deliver the different types of age assurance attributes and not all indicators of confidence for each type.

An age assurance service provider using biometrics techniques may have only been trained to provide the age assurance attribute type "over a certain age" for individuals over a specific age threshold or within a specific age range.

An age assurance service provider using specific documents to derive the age may only be able to provide the age assurance attribute type "over a certain age", e.g. for individuals over 18 or for individuals over 16.

This highlights the fact that indicators of confidence may be different upon the type of age assurance attribute that is required by the policy maker and the indicators of confidence that are requested by the relying party.

An age assurance system may support multiple indicators of confidence which could be dependent upon the underlying technique(s) being used.

6.2.1 Indicators of confidence for age verification systems

Some indicators of confidence may be directly dependent upon the type of document that contains the date of birth, e.g. whether it is a primary credential or a secondary credential, whether an original or a photocopy of it is being used and the kind of verification that is performed on that document to verify both its origin and its genuineness. Three different characteristics need to be considered.

The type of document being used may also depend upon the attribute value being checked; e.g. the same type of document will not necessarily be used for checking "Over 16" and "Over 60".

An Age Assurance Service Provider may need to refer to a different assurance policy depending upon the kind of checking being made and the indicator of confidence required.

The age check practice statement (clause 4.4) shall describe what is being done so that third parties (including policy makers) to enable them to make their own opinion in the accuracy and reliability of specific age assurance attributes and attribute value(s) and the indicators of confidence which are associated with them.

6.2.2 Indicators of confidence for age estimation systems

Such systems are usually deriving age assurance attributes using artificial intelligence (AI) to ascertain an age from one or more biometrics characteristics.

Such systems first need to be trained using a set a data that is representative of the population that could be checked.

The set of data being used may be dependant upon the age range being checked, the colour of the skin, gender or other human characteristics. Such systems first need to be trained using a set of data that is representative of the population that will be checked. To reduce bias against minorities and under-represented groups, the dataset should sufficiently represent the whole population, not just the largest segments of the population.

Furthermore in order to increase the accuracy, different set of training data can be used for some types of age assurance attributes and for some attribute values.

Biometrics systems using artificial intelligence (AI) exhibit both:

- a False Acceptance Rate (FAR): the percentage of identification instances in which persons that do not comply with the criteria are incorrectly accepted; and
- a False Rejection Rate (FRR): the percentage of identification instances in which persons that do not comply with the criteria are incorrectly rejected.

For a given biometric system, the crossover error rate (CER) is the point where the FAR crosses over with the FRR. A lower CER indicates that the biometric system is more accurate.

Beside the accuracy of the biometrics system, other factors need to be taken into consideration: the speed or throughput rate, and the acceptability to users.

Age assurance service providers shall refer to a different assurance policy depending upon the kind of checking being made.

The age check practice statement shall describe what is being done so that third parties (including policy makers) to enable them to make their own opinion in the accuracy and reliability of specific age assurance attributes and attribute value(s) and the set of indicators of confidence which are associated with them.

6.2.3 Indicators of confidence for age inference systems

Such techniques are usually deriving age attributes using a credential or a document that provides information which indirectly allows a decision that a natural person is over or under a certain age or within an age range.

As an example, the possession of a credit card usually demonstrates that the individual is over 18. However, the possession of that card does not assure that the possessor meets this condition.

The indicators of confidence may be directly dependent upon the type of document or the kind of object that is being possessed and the kind of verification that is performed on that document or object to verify both its origin and its genuineness.

The possession of one document or of one object only allows to make a check against a single attribute value.

If different type of documents or objects are being used the check will apply to different discrete values.

For each age assurance attribute and for each attribute value, age assurance service providers shall need to refer to a different assurance policy depending upon the kind of documents or objects being used and the checking being made.

The age check practice statement shall describe what is being done so that third parties (including policy makers) to enable them to make their own opinion in the accuracy and reliability of specific age assurance attributes and attribute value(s) and the set of indicators of confidence which are associated with them.

However, the age threshold value(s) will be directly dependent upon the type of document or the kind of credential that is being possessed and the kind of verification that is performed on that document or credential to verify both its origin and its genuineness.

The possession of one document or of one credential allows to make a check against one or two fixed age threshold values.

7 Privacy objectives

7.1 Privacy objectives for age assurance systems

Objectives that are applicable to age assurance systems, i.e. independently from the age verification, age estimation or age inference technique being used, are first introduced followed by objectives specific to age verification, age estimation and age inference techniques.

7.1.1 Non-disclosure of the date of birth

The objective is to prevent relying parties from knowing the date of birth of the natural person. If this objective is supported, the date of birth of the natural person shall not be communicated by the age assurance service provider.

This objective may be overridden by an external policy maker (clause 4.2) such as governmental, regulatory or authorising organisation, where disclosure of the date of birth is specifically required for compliance with their policy requirements.

NOTE: This objective is related to collection minimisation principle of ISO/IEC 29100.

7.1.2 Non-disclosure of the age

The objective is to prevent relying parties from knowing the age of the natural person based on a single request. If this objective is supported, the age of the natural person shall not be communicated by the age assurance service provider.

This objective may be overridden by an external policy maker (clause 4.2) such as governmental, regulatory or authorising organisation, where disclosure of the date of birth is specifically required for compliance with their policy requirements.

NOTE: This objective is related to collection minimisation principle of ISO/IEC 29100.

7.1.3 Unlinkability

The objective is to prevent relying parties from the ability to correlate transactions performed by the same individual on different services. If this objective is supported, the age assurance service provider shall identify how this property is being obtained.

NOTE: This objective is related to use, retention and disclosure limitation principle of ISO/IEC 29100.

7.1.4 Untraceability

When a third party is involved, the objective is to prevent the third party from knowing from which age assurance service provider the attributes (including age verification or age estimation) are to be presented by the individual. If this objective is supported, the solution shall identify how this property is being obtained.

NOTE: This objective is related to use, retention and disclosure limitation principle of ISO/IEC 29100.

7.1.5 Attributes minimisation

The objective is to restrict the amount of attributes disclosed by an individual to the minimum necessary to perform the transaction. If this objective is supported, the solution shall identify which attributes are being gathered by the age assurance service provider.

NOTE: This objective is related to collection minimisation principle of ISO/IEC 29100.

7.1.6 User awareness

The objective is to ensure that individuals have sufficient awareness, through the publication of an age check practice statement by the relying party or age assurance service provider of the process of age assurance. Sufficient and meaningful information shall be provided to the individual so that they can understand, in a format and language that can be reasonably expected to understand, which attributes will be released in the context of a given operation.

If this objective is supported, the solution shall identify how user awareness is being achieved.

Where a relying party is seeking to deploy measures to prevent and detect child sexual exploitation and abuse, a policy maker may determine that user awareness of the technique(s) used to achieve that objective would be counter-productive. In such cases, an age check practice statement may exclude such technique(s) from user awareness, but they shall, nevertheless, ensure compliance with relevant local regulations and laws about the deployment of such technique(s).

7.1.7 Conditional attribute exchange

[Appropriate text is required for this suggested additional clause].

7.2 Privacy objectives for age estimation systems

If biometric characteristics are being used to estimate the value of an age assurance attribute, the objective is to prevent the relying party from knowing the biometric characteristics of the natural person.

7.3 Privacy objectives for age inference systems

In age inference systems, a document or an object that provides information which indirectly implies that a natural person is over a certain age is being used.

The objective is to prevent relying party from knowing the exact content of that document or object related to the natural person.

EXAMPLE: if a credit card is being used, the brand of the credit card should not be communicated.

If social proofing is being used to estimate the value of an age attribute, the objective is to prevent the relying party from knowing the social networks that have been used.

8 Security objectives

8.1 Security objectives for age assurance systems

Objectives that are applicable to age assurance systems, i.e. independently from the age verification, age estimation or age inference technique being used, are first introduced followed by objectives specific to age verification, age estimation and age inference techniques.

These security objectives only apply when an age attribute needs to be presented remotely to a relying party. The age attribute can be obtained using age verification, age estimation or age inference.

The following security objectives have been identified:

(a) binding of an age determination attribute to the correct individual,

(b) detection of collusion attacks between individuals,

(c) detection of the freshness of an evidence by a relying party

(d) prevention of the forwarding of evidence by a relying party to another relying party

8.1.1 Binding of an age determination attribute to the correct individual

If the age attribute is obtained locally (e.g., by a door **supervisor** at the entrance of an area subject to age restrictions) using automated face equipment, then the binding with the correct individual is straightforward.

If the age attribute is obtained remotely (e.g., by a remote site) then the binding is not obvious.

In the context of a remote access, the binding to the age attribute should be done using one or more identifying attributes. If this objective is supported, the solution shall identify which identifying attribute(s) is/(are) being used or disclosed and how it/they will be used and verified by the relying party.

While it is easier when a software-only authenticator is used, the attack can succeed even if tamper proof hardware authenticator is used if biometric verification is not performed at the time of the use.

8.1.2 Detection of collusion attacks between individuals

If two individuals agree to collaborate and one of them obtains an age attribute, and if that individual transmits that attribute to another individual, that other individual shall not be able to use it. If this objective is supported, the solution shall identify how this control is being done.

8.1.3 Memorization of an age determination attribute by a remote site

If an individual has been recognized once to be over a certain age, a key question is whether such characteristic should be memorized or not by the relying party.

From an ease of use point of view, such memorization would be appreciated by the individuals.

If this objective is supported, the solution shall identify how this control is being done.

In order to obtain an enhanced indicator of confidence in the binding, additional techniques or methods can be used, but they might reveal private information.

8.1.4 Detection of the freshness of a credential by a relying party

The objective is to prevent the use by an individual of attributes contained in a credential indefinitely.

The credential shall either be associated with an explicit or an implicit validity period or shall contain a challenge previously generated by the relying party.

8.1.5 Forwarding of an attribute by an age assurance service provider to another provider only if allowed

If a relying party forwards to another relying party an age attribute security token that was intended for the first relying party. The second relying party shall be in a position to verify that the age attribute security token was effectively intended for itself. If this objective is supported, the solution shall identify how this control is being done.

8.2 Security objectives for age estimation systems

8.2.1 Biometric presentation attacks

Care should be taken to detect biometric presentation attacks. As an example, the liveliness of the individual should be checked so that still pictures are rejected.

If biometrics are being used, care should be taken to detect biometric presentation attacks. As an example, the liveness of the individual must be checked so that still pictures will be rejected.

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

Passive liveness detection doesn't need 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.

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.

9 Age assurance systems attack and contraindicators

9.1 General

Age assurance service providers shall recognise 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 outputs to relying parties

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

Age assurance services providers shall not be required to disclose their mechanisms to prevent attack vectors in their age check practice statement.

9.2 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 service providers should consider:

(a) the accuracy, trustworthiness, 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 or not a scalable attack can be monetised 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 repeatable
(d) the ease for collusion and complicity between parties (including between children and their parents or legal guardians)

(e) the impact of system vulnerabilities on the confidence in the age assurance attribute generated

9.3 Contraindicators

Age Assurance systems may deploy multiple age assurance components and may have multiple sources of information from both primary and secondary credentials. These may lead to mis-matches of data or information indicating that the claimed age may not be the true age. These are called contraindicators.

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

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

(b) communicate the existence of the contraindicator to each relying party

Bibliography

[1] ISO #####-#, *General title — Part #: Title of part*

[2] ISO #####-##:20##, *General title — Part ##: Title of part*

Annex A
(informative)

Guiding principles for relying party practice statement

A.1 Introduction

This annex provides additional guidance to assist relying parties when developing their practice statements and adopting acceptable approaches to age assurance. These guiding principles may also inform policy makers as they specify applicable types of Age Assurance Systems or related policy requirements.

A relying party practice statement has multiple purposes, both internal and external:

- Internally, a relying party can use the creation of their practice statement to determine the components of their age assurance system.
- Externally, the relying party practice statement communicates the procedures and practices employed by the relying party to individuals, policy makers, and age assurance service providers throughout the relying party's supply chain.

The variety of age assurance systems and sub-systems described in this standard present trade-offs between competing objectives. There is no one-size-fits all solution in this area. Instead, parties may opt for different approaches based on a variety of factors, including but not limited to users of the service, type of service offered, risk calculation, privacy expectations, and economic feasibility. The following guiding principles provide criteria and examples of specific procedures and practices that can be considered in order to fulfil the requirements for an age assurance relying party practice statement in 4.4.2.

When using these principles, relying parties should consider what aspects of their practice statement should be publicly disclosed per Clause 4.6, and what should be disclosed to policy makers or service providers.

A.2 Identify, evaluate, and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

Internal Aim: Ensure that a relying party engages in adequate forethought to the specific risks to youth, and incorporate insights into their practice statements.

Relying parties should evaluate risks that are specific to youth – for instance, content that may be inappropriate for younger users, or inappropriate contact from adults. Such risks and impacts are evaluated as products and features are developed, and they may evolve over time after a product or feature is launched. In turn, ongoing assessment and evaluation of risks and impacts is critical. They also assess how age assurance methods may impact both youth and other users.

Examples of specific practices to assess and analyse risks to youth when deploying age assurance include:

- Identify and categorize risks to youth related to content, conduct, contact with third parties, and commercial relationships made possible by a product or feature.
- Develop specialized expertise, insight, and analysis capabilities related to high-impact risks to youth and appropriate mitigation measures.
- Develop and implement frameworks and best practices for risk and impact assessment, which take into account, for instance, the likelihood of youth engaging with a service or feature; the audience the service is designed for; the evolving capacities of young people as they age; foreseeable risk; and the best interests of the young people.

- Consult third parties, including youth and families, in assessing risks and impacts, and selecting age assurance methods.
- Include experts in young people and their safety throughout the product development process, and provide for ongoing feedback both pre-launch and post-launch on risks to youth as well as upholding their rights.
- Structure these practices such that they can be shared with and described to auditors and researchers when appropriate.

Note on end user practice statements: The practices described in this section may not need to be disclosed to end users.

A.3 Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches.

Aim: Ensure that age assurance approaches respect data protection and privacy rights, including and especially the privacy rights of young people.

Relying parties should take into account privacy and data protection when evaluating what is most appropriate for a given feature or product. Each method of age assurance has different impacts on user privacy, and different services have different baseline privacy practices that impact user expectations.

Examples of specific practices to protect user privacy rights, which may aid the relying party in describing the age assurance provider approaches in their practice statement per Clause 4.2.2.e, include:

- Minimize collection of personal data for age assurance, in a manner proportionate to assessed risk, and design tailored practices regarding the retention, deletion, and use of data.
- Use sensitive data collected solely for age assurance only for that purpose, and delete such data expeditiously once a particular method is complete.
- Analyse personal data exclusively on-device wherever possible, to prevent its transmission to servers (including the digital service provider's servers) that are beyond the individual's control.
- Use age estimation methods on data that is already collected as a function of providing the service, to prevent collection of new personal data.
- Implement age assurance through a vendor such that any new personal data that is collected (e.g., a selfie photo) is only sent to the vendor that performs the age assurance test, not first to the digital service provider.
- Require that vendors apply high privacy and security standards, ensure appropriate third-party review and confirmation that those standards are met.
- Provide transparency to end-users about how their data is collected, used, and retained, with particular emphasis on the age assurance-related items listed above.
- Complete a Data Protection Impact Assessment before implementing any new age assurance method.
- Where possible, rely on interoperable age assurance solutions that minimize the burden on the user to provide additional information to new services, and mitigate the data protection risks the user must bear.

Note on end user practice statements: Except for the DPIA, the practices described in this section should be disclosed to end users in the practice statement.

A.4 Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.

Aim: Ensure age assurance does not unduly impede access to the service, taking into account the disparate impact that age assurance methods may have.

Age assurance would be counterproductive if it had the effect of eliminating access to services for wide swaths of users for whom those services are appropriate. Deploying an age assurance method that relies on, for example, a government-issued ID may have the effect of discriminating against younger users and users who've had no need to obtain a government-issued ID in their locale. Similarly, certain types of age estimation such as those based on facial images may have greater or lesser confidence levels for populations of a certain ethnicity or age demographic. A relying party should take these different effects on inclusivity into account when developing their practice statement.

Examples of specific practices to ensure inclusivity and accessibility for all users include:

- To the extent feasible and aligned with legal requirements, select age verification vendors that provide options beyond government-issued IDs, such as birth certificates and school IDs, or a combined unique account identifier and picture of the user, to ensure users without access to government-issued IDs are not discriminated against.
- Provide an accessible, easy-to-navigate appeals mechanism for those users who failed an age estimation test.
- Perform an impact analysis before deploying age estimation techniques to specific populations of users to understand any discriminatory outcomes and mitigate them.
- Provide a process for users to flag that a user is underage, and in concert with an enforcement action give that user in question access to an appeals process to prove their age.
- Conduct reviews of age assurance implementations, including with credentialed third-party vendors or service providers as appropriate.
- Consult with third parties to evaluate the impacts of age assurance methods under consideration.

Note on end user practice statements: Except for the third-party reviews and consultations, the practices described in this section should be disclosed to end users in the practice statement.

A.5 Conduct layered enforcement operations to implement age assurance approaches.

Aim: Ensure operational capacity exists to prevent users from accessing services or features that are inappropriate to the level of risk, limit access for those who are discovered to have accessed risk-inappropriate services or features, and to provide an appeals process for users whose access is impacted because of age assurance processes.

A relying party and/or policy maker may define and train an enforcement function within their organization that is equipped to implement policies on age-appropriate access based on the output of age assurance methods. Based on evaluations of risks, companies invest in a range of technologies and personnel to both select appropriate methods for age assurance and ensure their enforcement on an ongoing basis. These operations are "layered" in the sense that different approaches may be combined and different approaches may apply to different parts of a service, content, or features, based on levels of risk. Services also re-evaluate and adjust these operations based on evolving technologies and best practices.

These operations can be structured using the indicators of confidence in age assurance in Clause 6. Enforcement practices may also aid the relying party in describing the age assurance provider approaches in their practice statement per Clause 4.2.2.h.

Examples of specific practices of layered enforcement operations to implement age assurance approaches include:

- Set default limits on access to and discovery of the service, certain features, or particular content, subject to in-product notifications about age appropriateness of that content and/or some other form of age assurance.

- Label and, where appropriate, classify services as appropriate for only certain ages, and coordinate with distribution platforms to apply relevant limits for downloads and access by underage users.
- Deploy an age assurance check if a user changes their self-declared age from one that was <18 to an age >18.
- Analyse behaviour on a service for all users who self-declare an appropriate age at account creation, identifying users who may have inputted false information and are underage, and proactively putting these users through an additional age assurance test. Behaviour indicative of a self-declaration being inaccurate might be, for example, a message celebrating a user's own 11th birthday or repeated engagement with predominantly youth-directed content.
- Train enforcement teams to identify indicia of a user who has mis-reported their age (for instance, their appearance signals they are actually younger), and a method for triggering further age assurance.
- Allow users to report users who may have mis-reported their age and thus should be limited from the service or certain features.
- Implement technical methods that can help prevent users who have failed an age assurance test and been deemed ineligible from circumventing the controls (e.g., by immediately signing up with a different account).
- Apply new age assurance tests to existing users as a company improves or changes its assurance processes or makes relevant changes to a product or feature.
- Offer family accounts in connection with parental verification by attaching a young person's account to the parent's account.
- Empower users or community moderators to set age requirements for engagement with particular content or communities within a service.

Note on end user practice statements: Some aspects of the practices are built into the user experience and are encountered while interacting with the relying party; clearly identifying which experiences require an age-related eligibility threshold and setting default limits might be in this category and might not need to be separately described to end users in the practice statement. On the other hand, testing methods and analysis of contra-indicators would not typically be disclosed to an end user.

A.6 Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.

Aim: Ensure users and the public have insight into a service's age assurance methods.

Transparency serves a key function in informing the public and educating various stakeholders about a relying party's age assurance practices, while also building trust over time in the sufficiency of an industry's standard of care. At the same time, transparency needs to be considered alongside the risk of users figuring out how to game age assurance systems.

A relying party practice statement describes what age assurance practices should be disclosed to end users and what should be disclosed to other stakeholders, as well the means by which transparency can be communicated to these audiences.

Examples of specific practices to provide transparency about age assurance practices include:

- Explanations why age or birth date is collected as part of account sign-up.
- Implementation of open source age assurance solutions, such that the implementing code can be easily inspected by external stakeholders and experts.

- Providing third-party researchers access to implementation details and data on age assurance effectiveness such that evaluations of a given method's appropriateness can be made by external actors.
- Publishing data that explains the cost burden of different age assurance methods for providers of varying scale.
- Help center articles explaining a service provider's partnership with an age assurance vendor, including what data is shared and an overview of the vendor's data practices.
- Providing quantitative and qualitative information about enforcement of age assurance policies and practices.

Annex B
(informative)

Understanding indicators of confidence

An Age Assurance System may support multiple indicators of confidence. A scheme for indicators of confidence should be recognised in the jurisdiction, product category or service provision relevant to the use of an age related eligibility criteria.

An example of a scheme for indicators of confidence is provided in this Informative Annex.

Table 1 describes, in summary, the five core indicators of confidence as set out in clause 6.1.

Table 1 – Schematic: Indicators of Confidence in Age Assurance

Asserted	Basic	Standard	Enhanced	Strict
Based on self-asserted age attributes No validation or trust elevation deployed No attempt has been made to address contra indicators Could be utilised in low risk or only where indicative age is required Unlikely to be satisfactory for legally defined age-related eligibility	Based on self-asserted age attributes with a single age assurance component that has low confidence, but in combination is still likely to be correct at a rate of 9 times out of 10. Partial or simple validation or trust elevation; contra indicators may still be present Could be used for unregulated age gateways	Based on at least one age assurance component that satisfactorily provides confidence in being correct at a rate of 99 times out of 100. Validated and all contra indicators addressed Considered to be the minimum standard required for regulated age related eligibility unless a higher level is specified	Based on age assurance components that taken individually or combined satisfactorily provides confidence in being correct at a rate of 999 times out of 1000. Validated and all contra indicators addressed Likely to be useful for enhanced risk goods, content or services age-related eligibility	Based on a combination of age assurance components that satisfactorily provides confidence in being correct at a rate of 9999 times out of 10000. Validated and all contra indicators addressed Likely to be useful where age-related eligibility is critical to safeguarding or protecting against child sexual exploitation or abuse

To achieve any given indicators of confidence, the age assurance process should meet at least each of the minimum requirements for that indicator. It may exceed the minimum in some dimensions but the indicators of confidence achieved are determined by the lowest achievement on any dimension.

The approaches to measurement and testing of age assurance could be structured around these indicators of confidence.

However, policy makers, relying parties and age assurance service providers may identify a need to sub-divide these indicators of confidence to provide greater granularity for a particular use case. Additionally, policy makers, relying parties and age assurance service providers may determine that age assurance attributes with some indicators of confidence either can not or could not be applicable to a particular age-related eligibility decision.

SUGGESTIONS FOR INCLUSION AS DIAGRAMS

Editor's Note: At the 42nd Meeting of ISO/IEC JTC 1/SC 27/WG 5, experts suggested that Clause 4.1 of the document would be aided by some diagrams. A number of options and styles have been suggested and these are included below. Contributions are invited on these suggestions and any alternate suggestions that contributors may wish to propose.

This section will be removed from the CD and adopted diagrams placed in line with the appropriate text and position in the document.

There are 14 different options presented, the Editor considers that approximately 3 or 4 may be required in the final document.

Figure 1: High level description of actors in an age assurance process

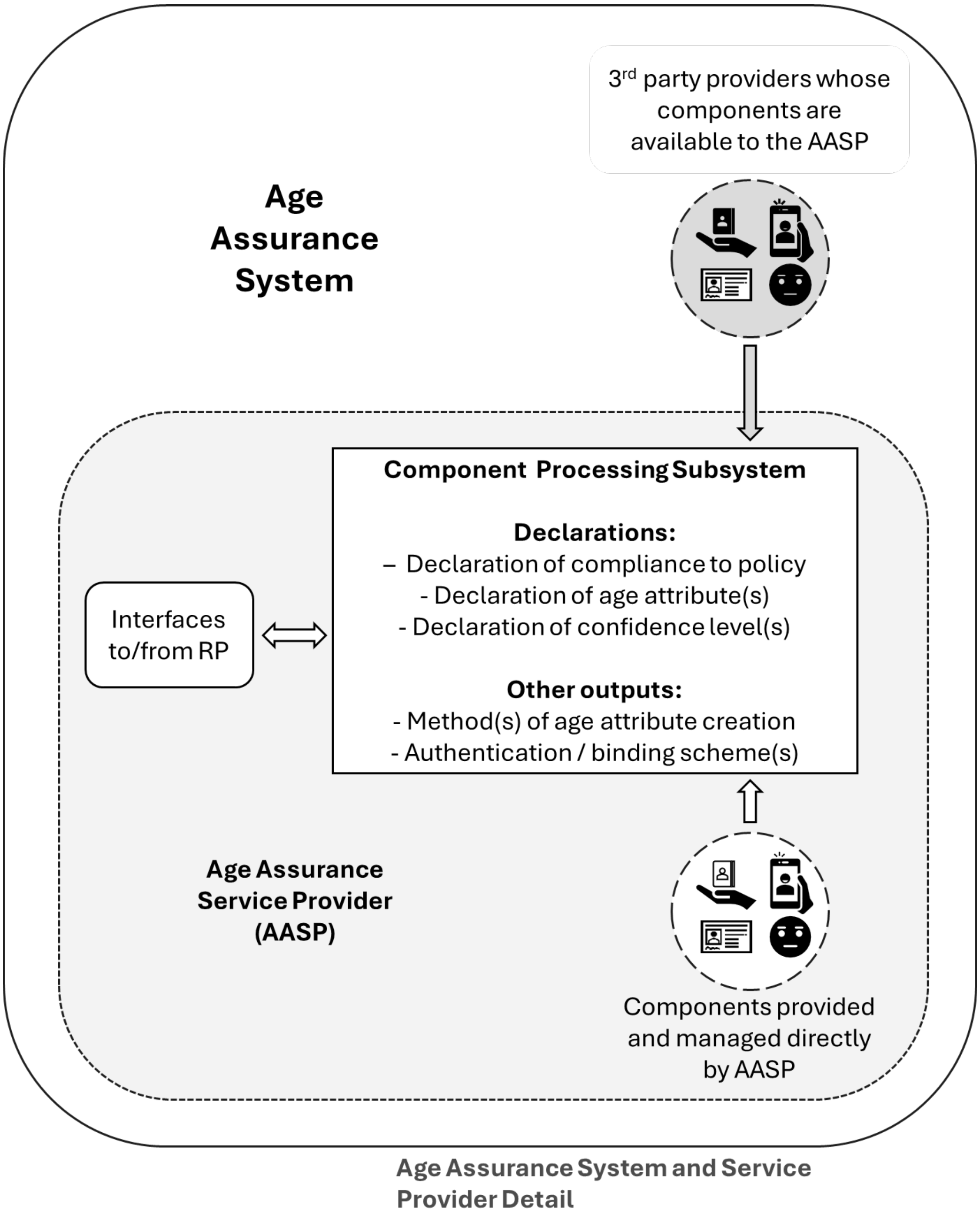

3rd party providers whose components are available to the AASP
Age Assurance System
Component Processing Subsystem
Declarations:
– Declaration of compliance to policy
- Declaration of age attribute(s)
- Declaration of confidence level(s)
Other outputs:
- Method(s) of age attribute creation
- Authentication / binding scheme(s)
Interfaces to/from RP
Age Assurance Service Provider (AASP)
Components provided and managed directly by AASP
Age Assurance System and Service Provider Detail

Figure 2: Process flow for age related eligibility decisions

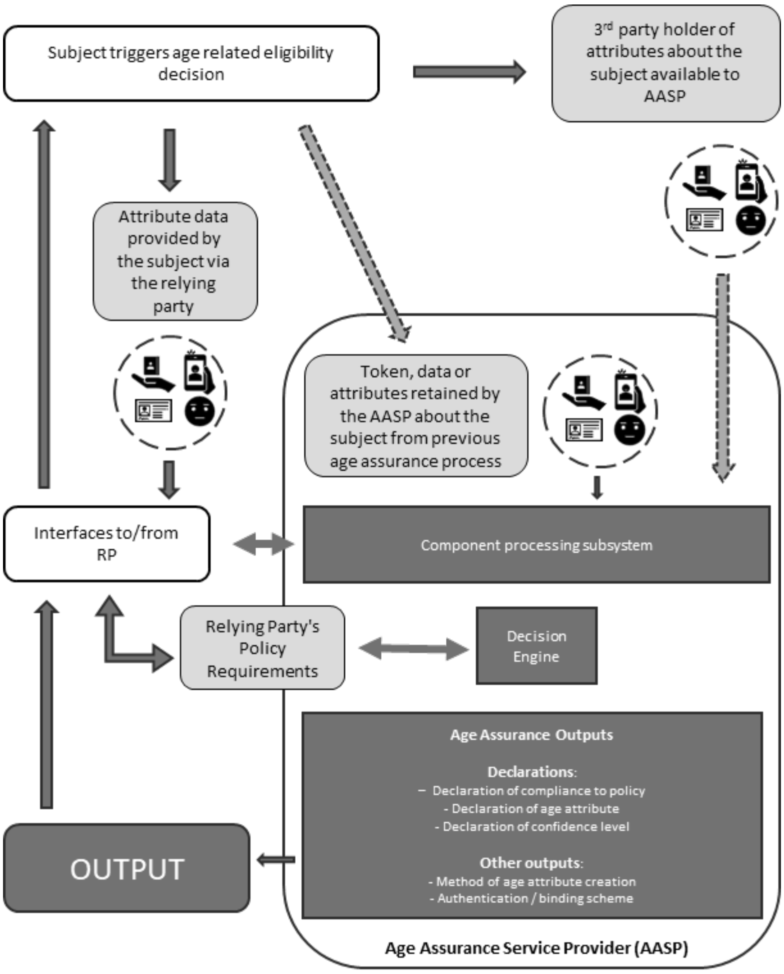

Subject triggers age related eligibility decision
3rd party holder of attributes about the subject available to AASP
Attribute data provided by the subject via the relying party
Token, data or attributes retained by the AASP about the subject from previous age assurance process
Interfaces to/from RP
Component processing subsystem
Relying Party's Policy Requirements
Decision Engine
Age Assurance Outputs
Declarations:
– Declaration of compliance to policy
- Declaration of age attribute
- Declaration of confidence level
Other outputs:
- Method of age attribute creation
- Authentication / binding scheme
OUTPUT
Age Assurance Service Provider (AASP)

Figure 3: Relationships between contracting parties in an age assurance process

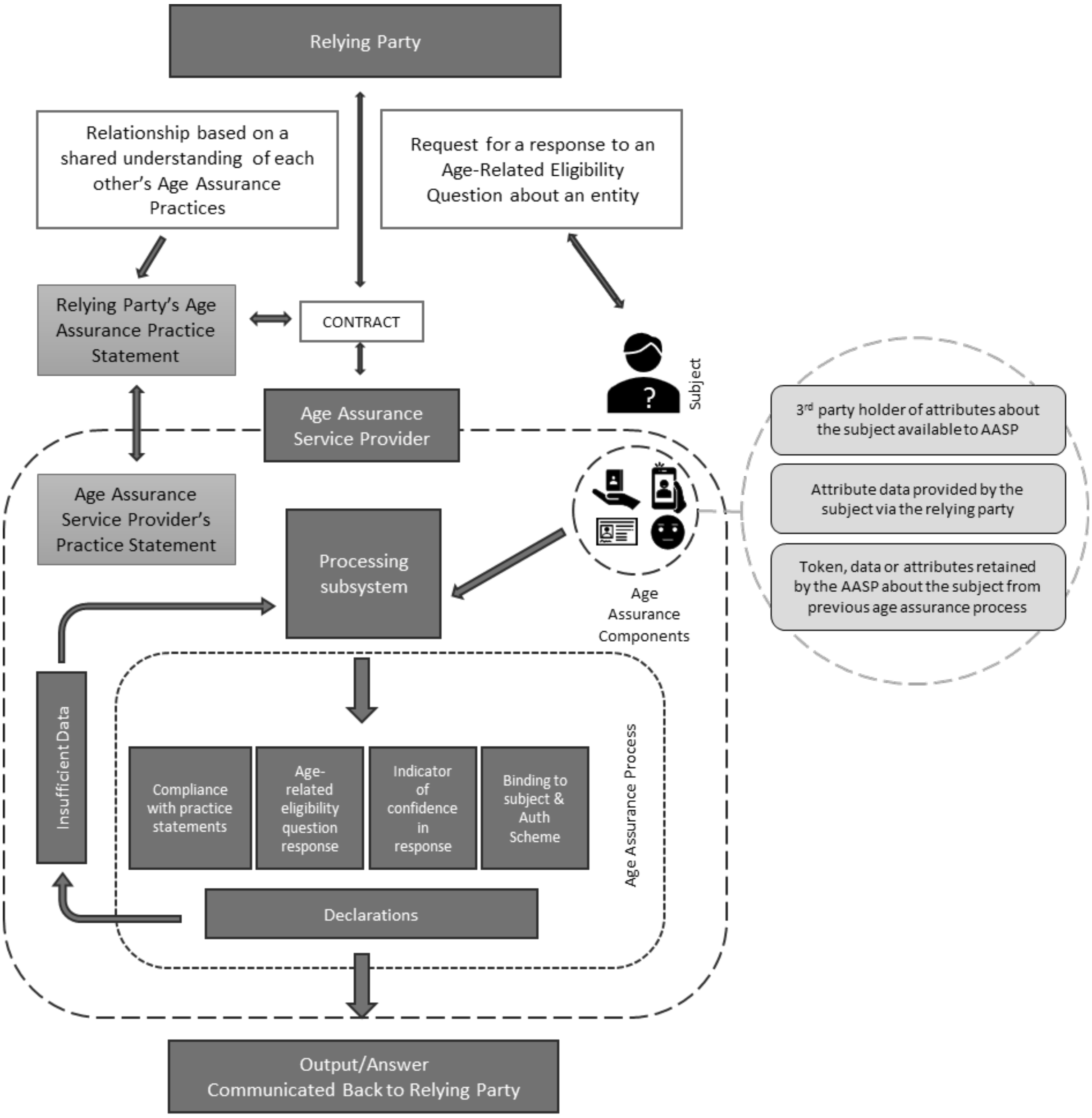

Relying Party
Relationship based on a shared understanding of each other's Age Assurance Practices
Request for a response to an Age-Related Eligibility Question about an entity
Relying Party's Age Assurance Practice Statement
CONTRACT
Subject
Age Assurance Service Provider
Age Assurance Service Provider's Practice Statement
Processing subsystem
Age Assurance Components
3rd party holder of attributes about the subject available to AASP
Attribute data provided by the subject via the relying party
Token, data or attributes retained by the AASP about the subject from previous age assurance process
Insufficient Data
Compliance with practice statements
Age-related eligibility question response
Indicator of confidence in response
Binding to subject & Auth Scheme
Age Assurance Process
Declarations
Output/Answer Communicated Back to Relying Party

Figure 4: Ecosystem of age assurance services

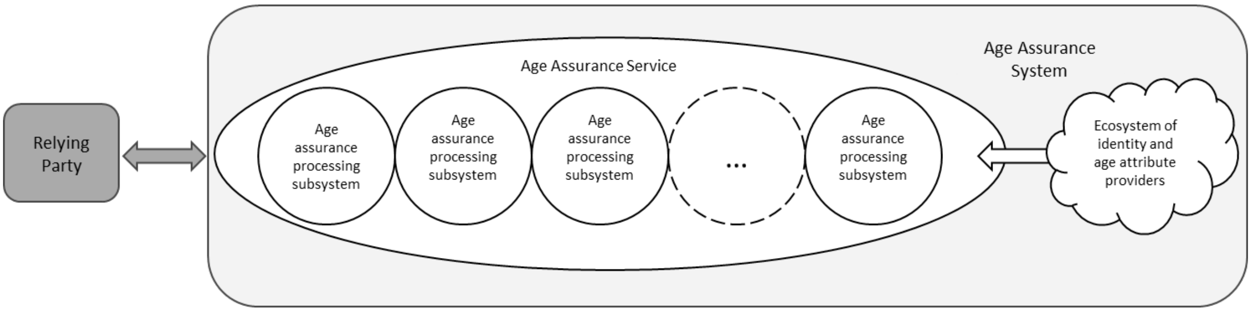
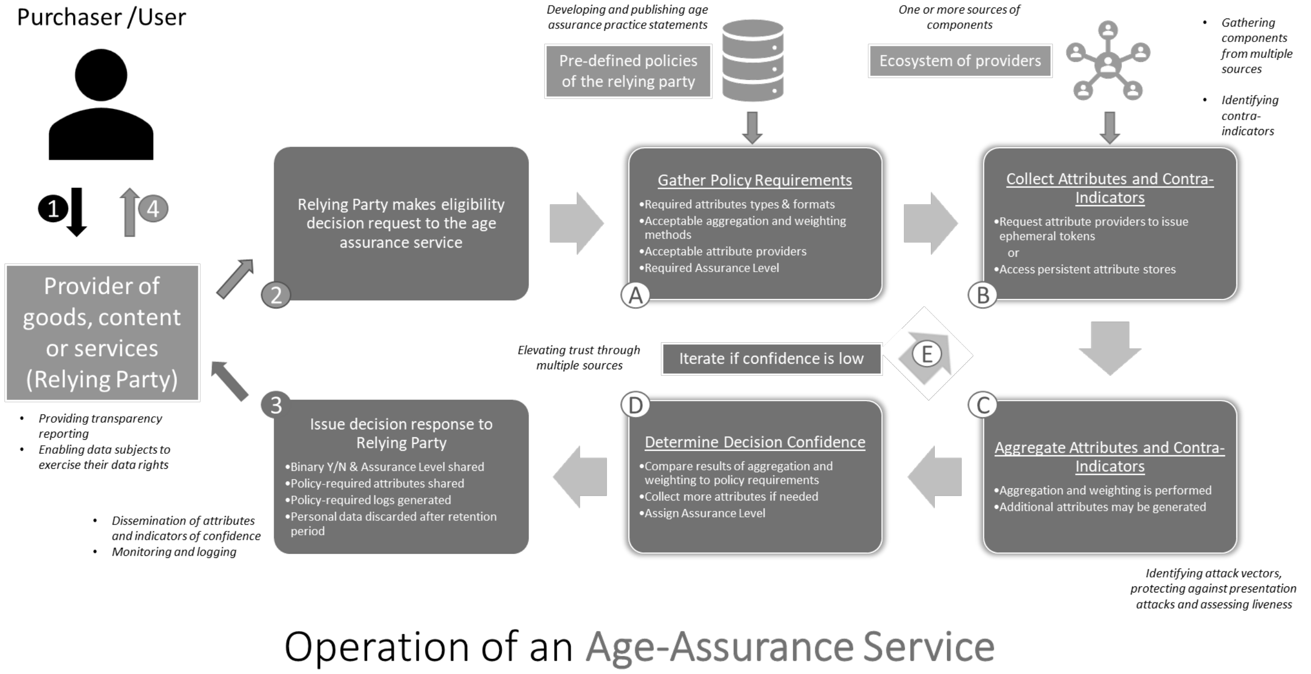

Relying Party
Age Assurance Service
Age Assurance System
Age assurance processing subsystem
Age assurance processing subsystem
Age assurance processing subsystem
...
Age assurance processing subsystem
Ecosystem of identity and age attribute providers

Figure 5: Operation of an age assurance service



Provider of goods, content or services (Relying Party)

- Providing transparency reporting
- Enabling data subjects to exercise their data rights

Relying Party makes eligibility decision request to the age assurance service

Developing and publishing age assurance practice statements

Pre-defined policies of the relying party

Gather Policy Requirements

- Required attributes types & formats
- Acceptable aggregation and weighting methods
- Acceptable attribute providers
- Required Assurance Level

One or more sources of components

Ecosystem of providers

- Gathering components from multiple sources
- Identifying contra-indicators

Collect Attributes and Contra-Indicators

- Request attribute providers to issue ephemeral tokens
  or
- Access persistent attribute stores

Elevating trust through multiple sources

Iterate if confidence is low

Aggregate Attributes and Contra-Indicators

- Aggregation and weighting is performed
- Additional attributes may be generated

Identifying attack vectors, protecting against presentation attacks and assessing liveness

Determine Decision Confidence

- Compare results of aggregation and weighting to policy requirements
- Collect more attributes if needed
- Assign Assurance Level

Issue decision response to Relying Party

- Binary Y/N & Assurance Level shared
- Policy-required attributes shared
- Policy-required logs generated
- Personal data discarded after retention period

- Dissemination of attributes and indicators of confidence
- Monitoring and logging

Operation of an Age-Assurance Service

Explanatory Note for Figure 5:

1. It can be iterative, especially for age assurance. At the binary decision stage the decision could be a "confidence level is too so escalate to a different set of attributes & providers". This would be an arrow in the flow from the last step back to either the policy or provider step (steps 2 & 3) For example if using AI we can estimate age sufficiently (like a bartender at a bar) then we have a high confidence that our requirement is met (">18 years old") and we're done. If our confidence isn't high enough with just AI we can go back to a document-based age assurance via id verification

The last step could return more than just a Y/N decision and will often be done by the resource server. In the case of age assurance we often want a full date of birth, at least for 'children' (due to e.g. children gaining certain digital rights at certain ages esp in the EU - we can't deny those rights for 6-12 months because we only have age and not dob). This is why MSA creation requires full dob. So the resource server may get a set of verified claims as a result then make a set of decisions based on those claims (e.g. imagine if Xbox hid all Mature games from <13yr children but would allow them to see but not play Teen-rated games - that's >1 decision based on 1 attribute claim)

Figure 6: Example of age assurance process in digital safety laws

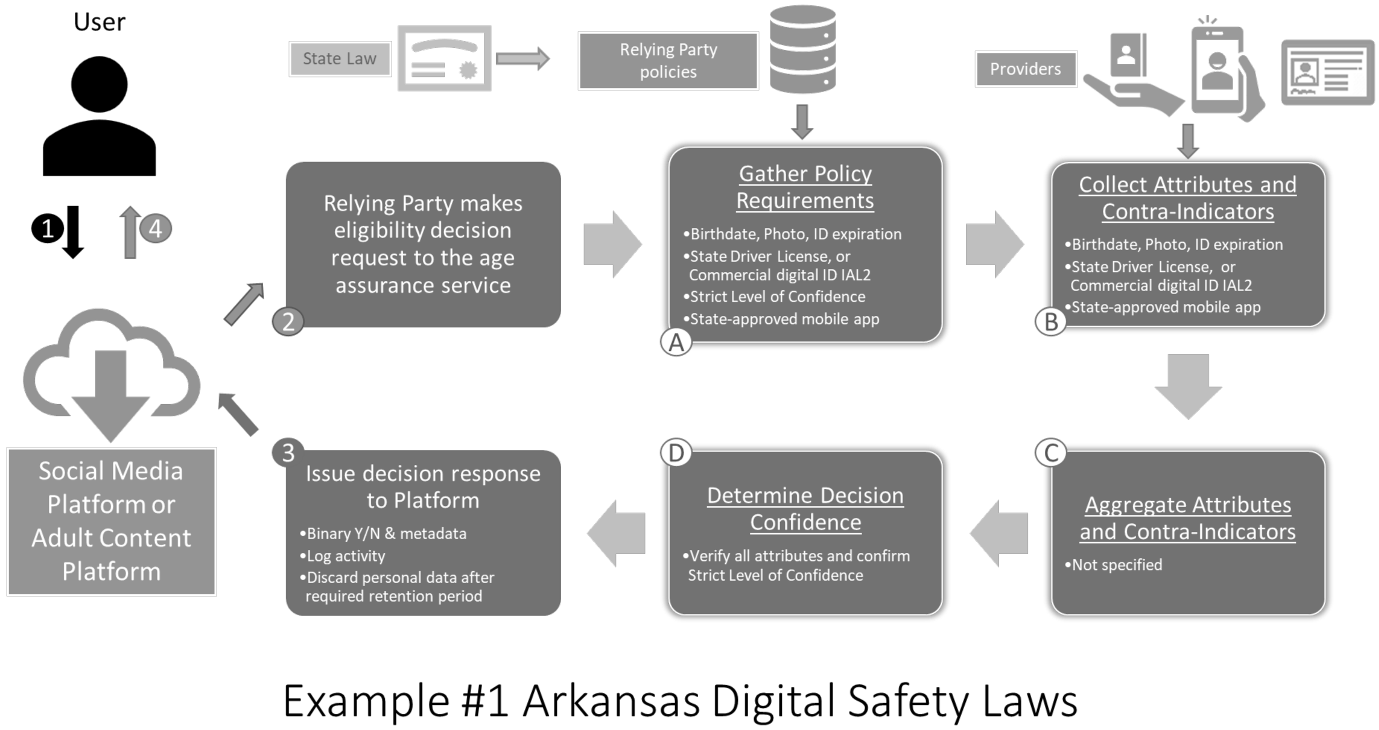

User
1
4
Social Media Platform or Adult Content Platform
State Law
Relying Party policies
Providers
2
Relying Party makes eligibility decision request to the age assurance service
Gather Policy Requirements
•Birthdate, Photo, ID expiration
•State Driver License, or Commercial digital ID IAL2
•Strict Level of Confidence
•State-approved mobile app
A
Collect Attributes and Contra-Indicators
•Birthdate, Photo, ID expiration
•State Driver License, or Commercial digital ID IAL2
•State-approved mobile app
B
3
Issue decision response to Platform
•Binary Y/N & metadata
•Log activity
•Discard personal data after required retention period
D
Determine Decision Confidence
•Verify all attributes and confirm Strict Level of Confidence
C
Aggregate Attributes and Contra-Indicators
•Not specified
Example #1 Arkansas Digital Safety Laws

Figure 7: Example of age assurance process in retail environment

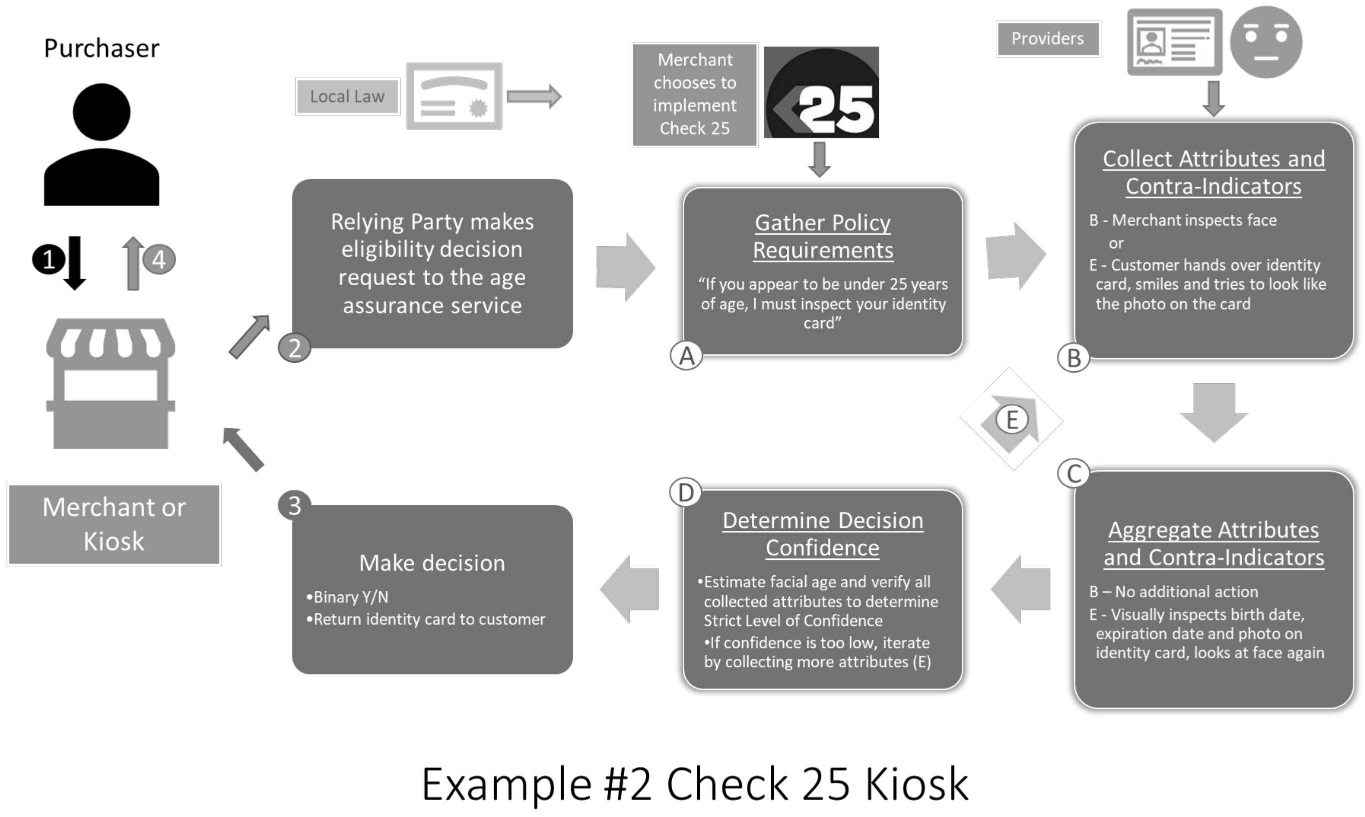

Purchaser
1
4
Merchant or Kiosk
Local Law
Merchant chooses to implement Check 25
25
Providers
2
Relying Party makes eligibility decision request to the age assurance service
Gather Policy Requirements
"If you appear to be under 25 years of age, I must inspect your identity card"
A
Collect Attributes and Contra-Indicators
B - Merchant inspects face
or
E - Customer hands over identity card, smiles and tries to look like the photo on the card
B
E
3
Make decision
•Binary Y/N
•Return identity card to customer
D
Determine Decision Confidence
•Estimate facial age and verify all collected attributes to determine Strict Level of Confidence
•If confidence is too low, iterate by collecting more attributes (E)
C
Aggregate Attributes and Contra-Indicators
B – No additional action
E - Visually inspects birth date, expiration date and photo on identity card, looks at face again
Example #2 Check 25 Kiosk

Figure 8: A high level description of the key actors involved in the process

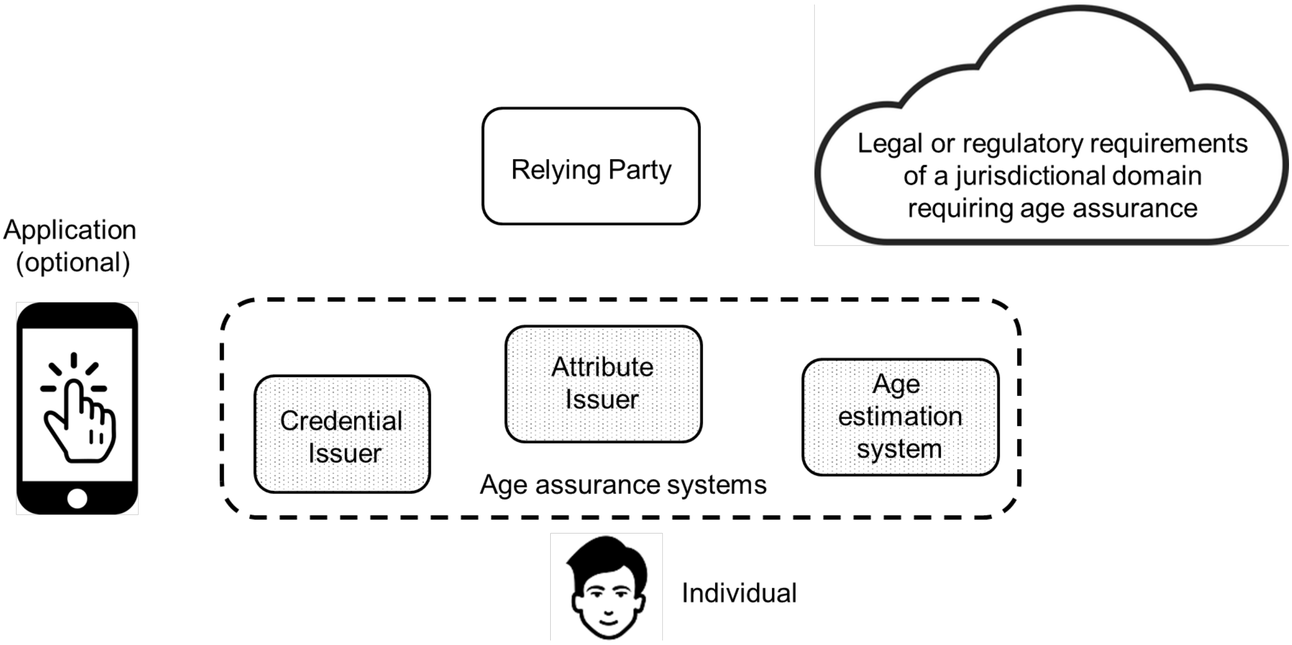


Figure 9: A process flow diagram for triggering of an age related eligibility decision for age verification and age estimation supported using an on-line age assurance system at the time of the request

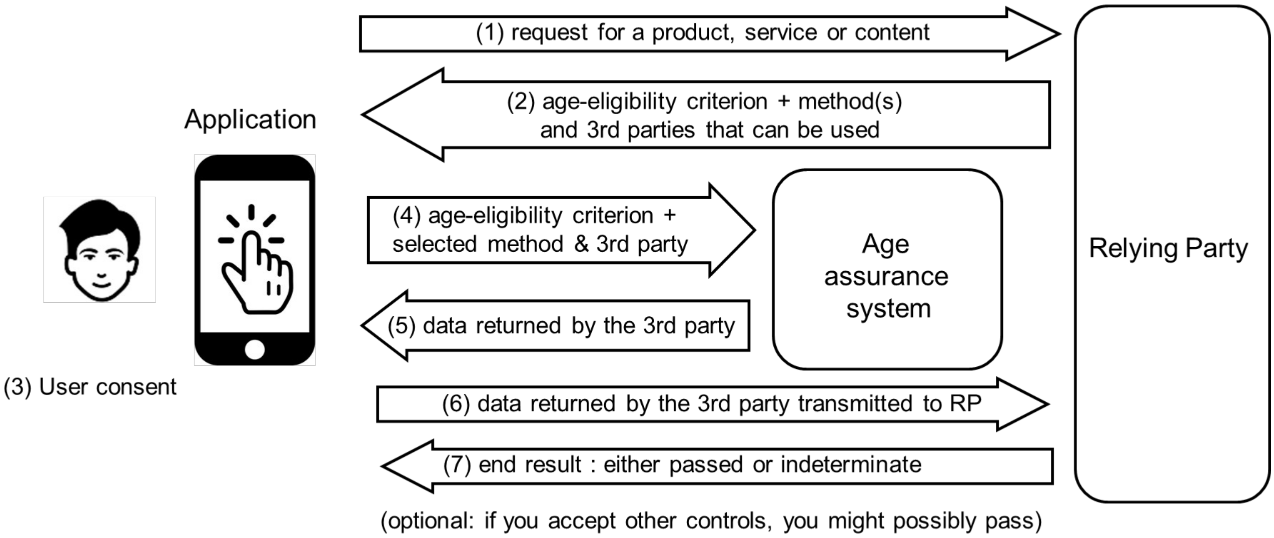

(1) request for a product, service or content
(2) age-eligibility criterion + method(s) and 3rd parties that can be used
Application
(4) age-eligibility criterion + selected method & 3rd party
Age assurance system
Relying Party
(5) data returned by the 3rd party
(3) User consent
(6) data returned by the 3rd party transmitted to RP
(7) end result : either passed or indeterminate
(optional: if you accept other controls, you might possibly pass)

Figure 10: A process flow diagram for triggering of an age related eligibility decision for age verification supported using data locally derived from credentials obtained prior to the request

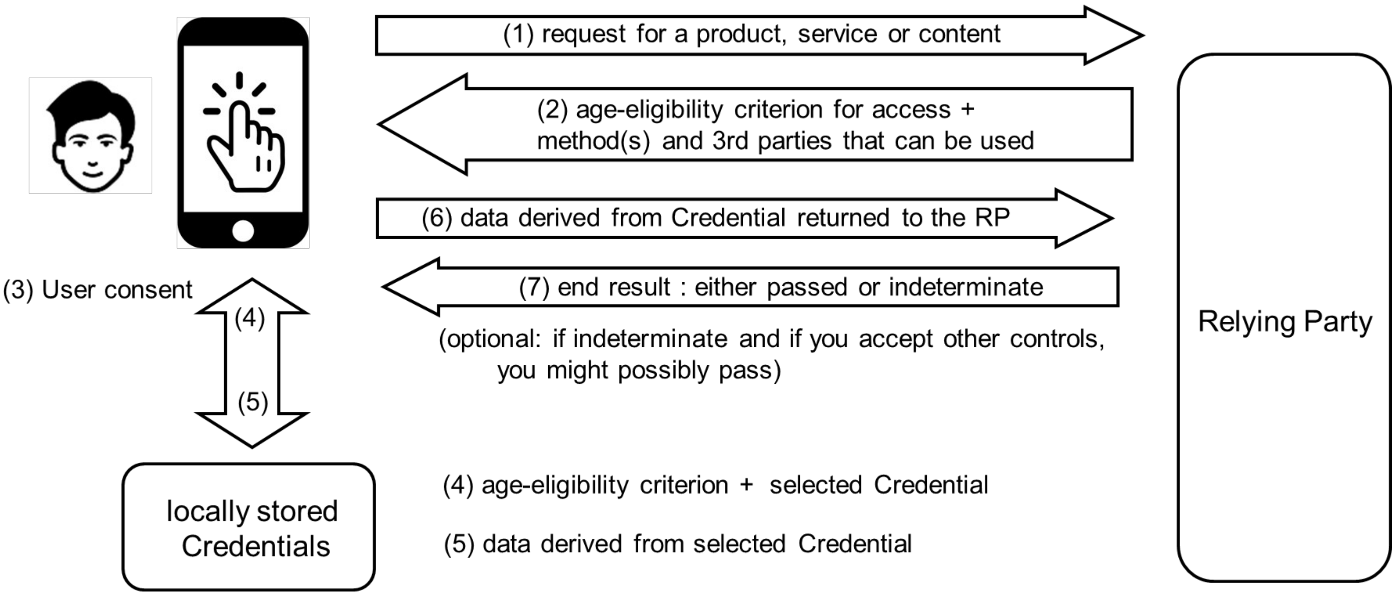

(1) request for a product, service or content
(2) age-eligibility criterion for access + method(s) and 3rd parties that can be used
(6) data derived from Credential returned to the RP
(7) end result : either passed or indeterminate
(optional: if indeterminate and if you accept other controls, you might possibly pass)
Relying Party
(3) User consent
(4)
(5)
locally stored Credentials
(4) age-eligibility criterion + selected Credential
(5) data derived from selected Credential

Figure 11: A process flow diagram for triggering of an age related eligibility decision for age estimation supported using a system that performs a facial analysis when the Relying Party is not accessible through the Internet and the individual is not using an application

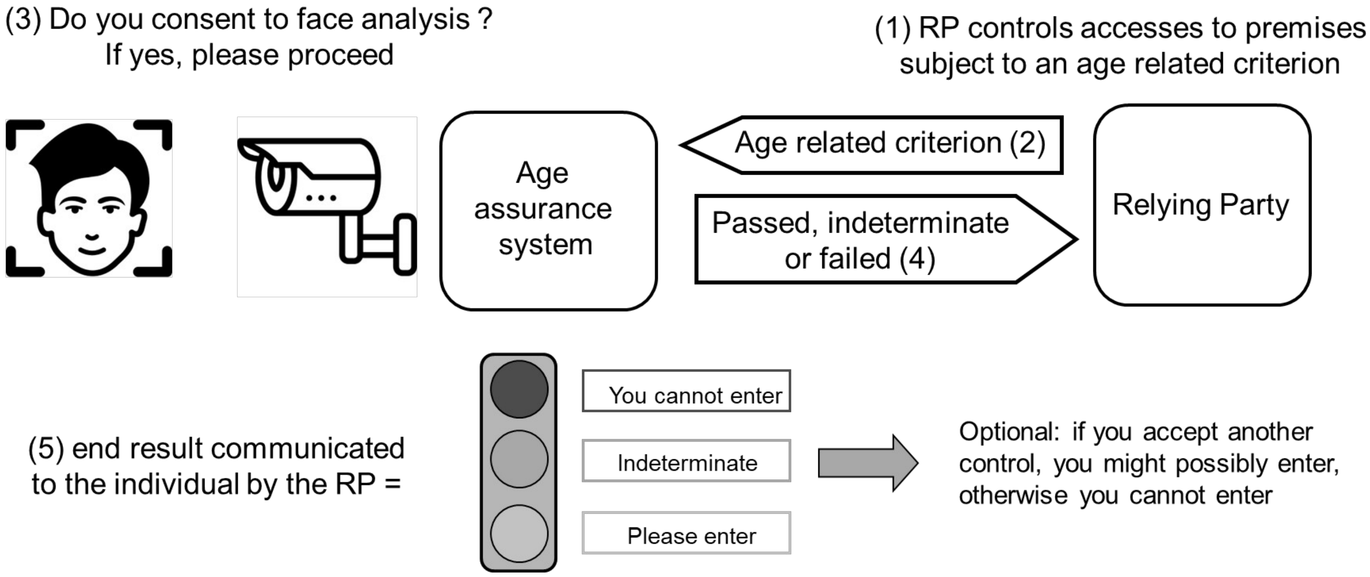

(3) Do you consent to face analysis ? If yes, please proceed
(1) RP controls accesses to premises subject to an age related criterion
Age assurance system
Age related criterion (2)
Passed, indeterminate or failed (4)
Relying Party
(5) end result communicated to the individual by the RP =
You cannot enter
Indeterminate
Please enter
Optional: if you accept another control, you might possibly enter, otherwise you cannot enter

Figure 12: Contracts and relationships diagram between the parties

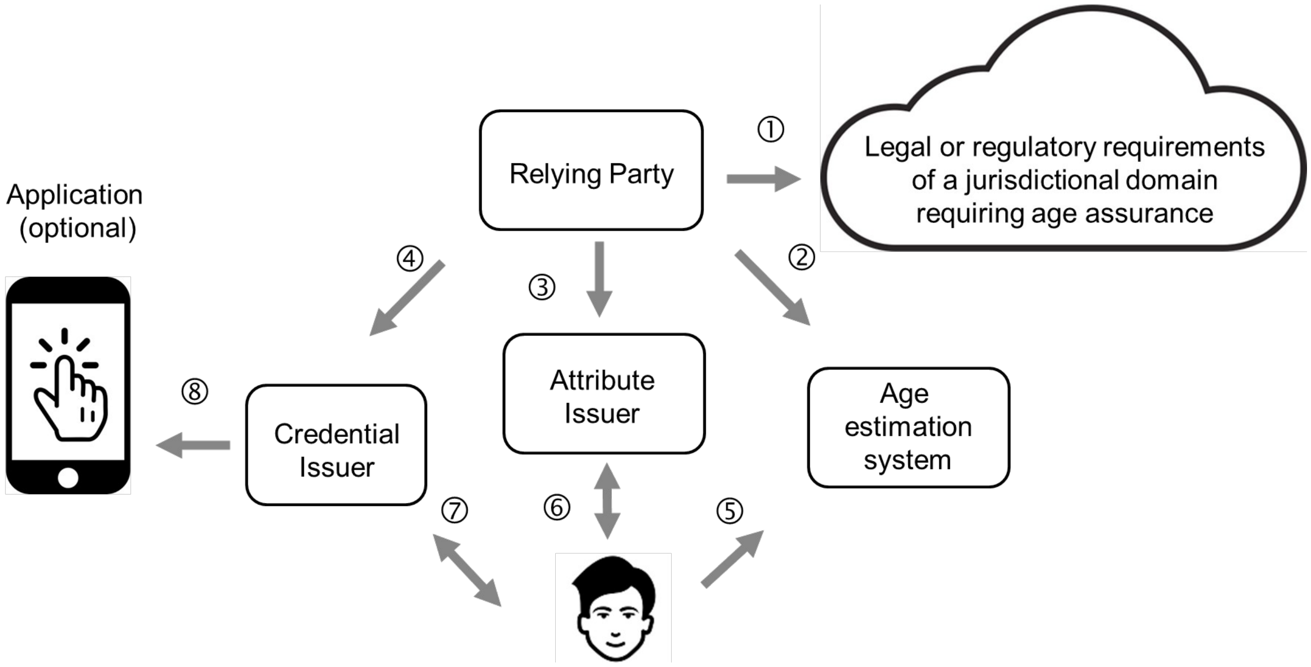
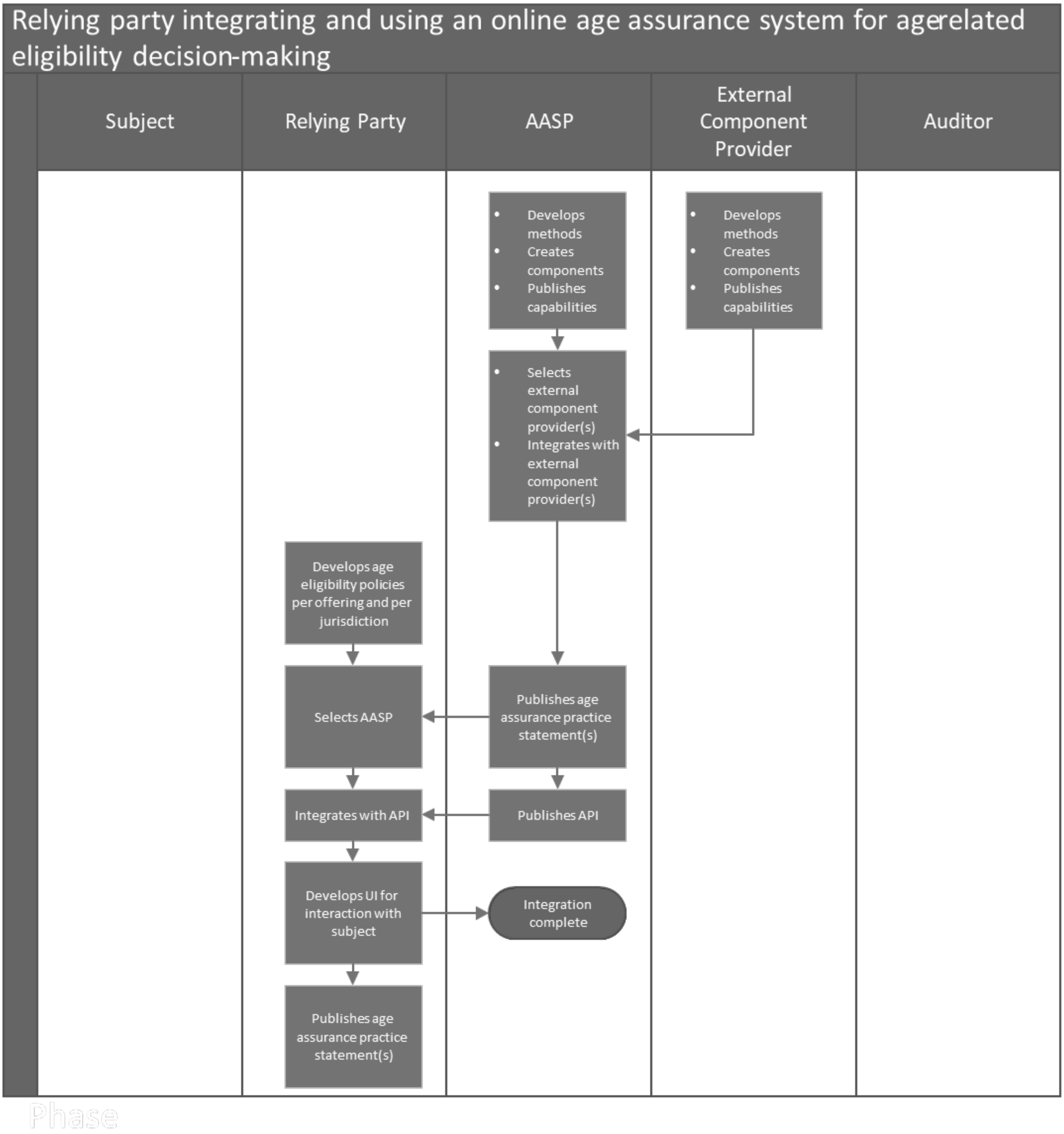
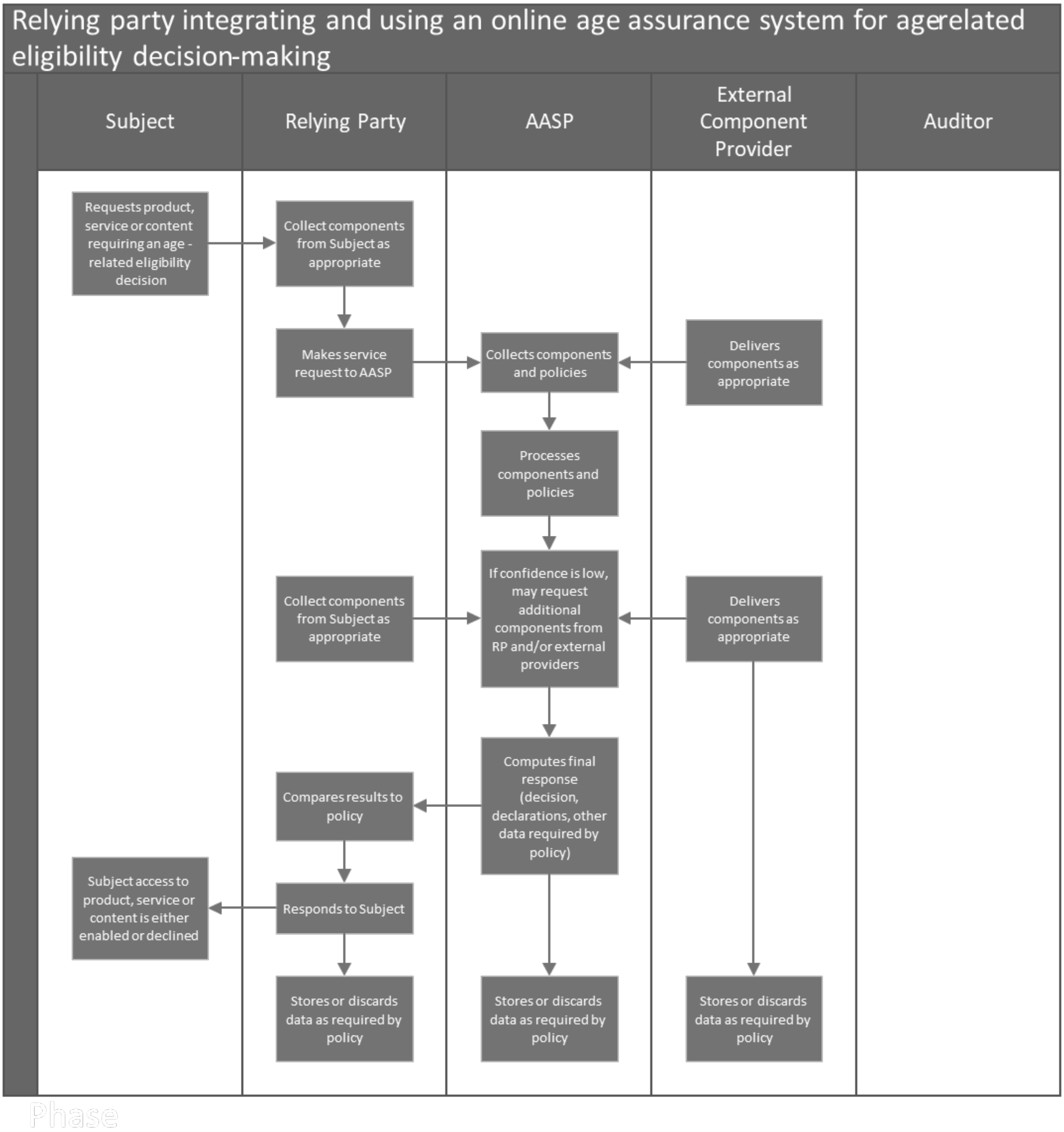


Figure 13: Swim lanes diagram for integrated online age assurance system


Relying party integrating and using an online age assurance system for agerelated eligibility decision-making
Subject
Relying Party
AASP
External Component Provider
Auditor
Develops methods
Creates components
Publishes capabilities
Develops methods
Creates components
Publishes capabilities
Selects external component provider(s)
Integrates with external component provider(s)
Develops age eligibility policies per offering and per jurisdiction
Selects AASP
Publishes age assurance practice statement(s)
Integrates with API
Publishes API
Develops UI for interaction with subject
Integration complete
Publishes age assurance practice statement(s)
Phase

1 **Figure 14: Swim lanes diagram for age related decision making**


Relying party integrating and using an online age assurance system for agerelated eligibility decision-making
Subject
Relying Party
AASP
External Component Provider
Auditor
Requests product, service or content requiring an age - related eligibility decision
Collect components from Subject as appropriate
Makes service request to AASP
Collects components and policies
Delivers components as appropriate
Processes components and policies
Collect components from Subject as appropriate
If confidence is low, may request additional components from RP and/or external providers
Delivers components as appropriate
Computes final response (decision, declarations, other data required by policy)
Compares results to policy
Subject access to product, service or content is either enabled or declined
Responds to Subject
Stores or discards data as required by policy
Stores or discards data as required by policy
Stores or discards data as required by policy
Phase

2