



**CAN/DGSI 127:2025**  
**NATIONAL STANDARD OF CANADA**

**First Edition**  
**2025-08**

**Age Assurance Technologies**

35.020; 35.030; 35.240.99



- Page left intentionally blank -

## Table of Contents

<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>1</b>
<b>Context</b> .....	<b>3</b>
<b>1 Scope</b> .....	<b>5</b>
<b>2 Normative References</b> .....	<b>5</b>
<b>3 Terms and Definitions</b> .....	<b>5</b>
<b>4 Age assurance process</b> .....	<b>7</b>
<b>5 Compliance and risk assessment</b> .....	<b>7</b>
<b>6 Selection of age assurance method</b> .....	<b>8</b>
<b>7 Design of age assurance technology</b> .....	<b>9</b>
<b>8 Undertake age assurance</b> .....	<b>10</b>
<b>Bibliography</b> .....	<b>12</b>

- Page left intentionally blank -

## Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organizations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

**Digital Governance Standards Institute**

500-1000 Innovation Dr.

Ottawa, ON K2K 3E7

[www.dgc-cgn.org](http://www.dgc-cgn.org)

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at [www.scc.ca](http://www.scc.ca).

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at [www.scc.ca](http://www.scc.ca).

- Page left intentionally blank -

## Introduction

This is the First Edition of CAN/DGSI 127:2025, Age Assurance Technologies.

CAN/DGSI 127:2025 was prepared by the DGSI Technical Committee 18 (TC 18) on Age Assurance, comprised of over 45 thought leaders and experts in the design, and use of age assurance technologies. This Standard was approved by a Technical Committee formed balloting group, comprised of 4 producers, 4 government / regulator / policymakers, 2 users, and 4 general interests.

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than two years from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

This Standard is intended to be used for conformity assessment.

ICS 35.020; 35.030; 35.240.99

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

- Page left intentionally blank -

## Context

*Age assurance* is an umbrella term for different methods used to calculate a person's age or age range, including *age verification* and *age estimation* methods which offer varying levels of certainty. Historically, attempts to restrict access based on age-gating methods such as asking a person to indicate their date of birth or that they are over the age of majority, have been unreliable as they are easily bypassed – a service provider cannot know if the person is telling the truth, and some parental controls can be bypassed through third-party apps.

Online access to adult content, services, transactions or interactions have put minors at risk of physical and mental harm. These online safety risks for minors can be grouped into four areas: Content, Contact, Conduct and Contract.

The existing range of technical protection measures to control access based on one's age is vast and might rely on other various technologies. Some commonly used methods are as follows. Note that these measures *should* be integrated with other processes/measures to protect minors and to control access to services, and each measure carries a varying level of risk for the individual.

1. Self-check: *Users* are asked to declare their ages while agreeing to the terms of usage of the service.
2. Document-based verification: *Users* are asked to present digital versions of authorized identification documents (e.g. driving licenses, health cards, passports, proof of age cards) to prove their ages. This has been the most common method so far for online *age verification*.
3. Biometric and characteristic based verification: Detection and analysis of biological and characteristic features of humans that vary with age.
4. Capacity testing: Capacity testing allows a service to estimate a *user's* age based on an assessment of their aptitude or capacity. For example, a minor may be asked to complete a language test, solve a puzzle, or undertake a task that serves as an indication of their age or age range.
5. Cross-account or cross-platform authentication: *Users* can verify their ages through an existing verified account in another domain or through a third party (such as a credit card or reusable digital ID), through which their ages get cross-checked.
6. Profiling: Profiling refers to the process of analysing the behaviour of *users* to predict their ages. Data used for profiling consists of information that *users* choose to share about themselves and information that is automatically collected from their engagement with services.
7. Authorized confirmation: An adult account holder (i.e., parent or guardian) is either asked to confirm the age of the minor *user* or asked to create a special account for the minor. In both scenarios, the adult takes responsibility for verifying the age of the minor. This may be a parent, or to add independence, a recognised professional.

Certifying *age assurance* technologies and processes against consensus-based standards can provide added confidence and assurance that the design, use, and accuracy of such technologies is reliable; maintains *users'* privacy and protects their *personal information*; limits collection and use of *personal*

*information* to the entity collecting the information solely for *age assurance* purposes; that all *personal information* collected for *age assurance* purposes is securely destroyed when the assurance process is completed; and that the *age assurance* processes, technologies, and practices comply with privacy laws.

This standard focuses explicitly on the role of *age assurance* technologies in facilitating a *user's* cyber-safety and articulates how best to implement *age assurance* in a manner that is privacy preserving, secure, effective, efficient, and easy-to-use. Note that there might be additional considerations that work in tandem with *age assurance* approaches, such as parental control and consent.

## Age Assurance Technologies

### 1 Scope

This standard specifies minimum requirements for *age assurance* technologies and methods to estimate or verify a person's age or their age range.

This standard is platform-agnostic.

### 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 27566-1, Information security, cybersecurity and privacy protection — Age assurance systems – Part 1 – Framework*

*Pan-Canadian Trust Framework - Privacy, Digital ID & Authentication Council of Canada*

### 3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply:

**age assurance**

Set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make age-related eligibility decisions with varying degrees of certainty.

[SOURCE: ISO/IEC 27566-1]

**age assurance provider**

Entity responsible for providing *age assurance results* to a *Relying Party*.

[SOURCE: ISO/IEC 27566-1]

**age assurance result**

Information produced by an *age assurance* system indicating that an individual is a certain age, over or under a certain age or within an age range.

[SOURCE: ISO/IEC 27566-1]

**age estimation**

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

[SOURCE: ISO/IEC 27566-1]

**age-restricted**

Limited to people above or below a certain age.

**age verification**

Age *assurance* method based on calculating the difference between a verified year or date of birth of an individual and a subsequent date.

NOTE: In some cultures, an alternate calculation (such as use of birth year rather than birth date) may be applicable.

[SOURCE: ISO/IEC 27566-1]

**data minimization**

A data controller *should* limit the collection of *personal information* to what is directly relevant and necessary to accomplish a specified purpose. They *should* also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers *should* collect only the personal data they really need and *should* keep it only for as long as they need it.

[SOURCE: European Data Protection Supervisor's Glossary of Data Protection Terms]

**personal information**

Any information that relates to an identifiable individual.

**personally identifiable information**

See *personal information*.

**privacy by default**

The principle that by default, ensures privacy settings are automatically set to the highest level of protection for *users*.

**privacy by design**

The principle that organizations *should* consider privacy and data protection concerns when designing, building and using products and services.

**relying party**

An entity that relies on an *age assurance result* to make an age-related eligibility decision.

NOTE: The *Relying Party* could also be an operating system, a platform or a device.

**robustness**

The degree to which an *age assurance* method can correctly determine the age of a *user* in actual deployment contexts.

**security by design**

The principle that organizations *should* consider security and data protection concerns when designing, building and using products and services.

**shall**

A requirement.

**should**

A recommendation.

**user / user party**

Individual who wishes to access *age-restricted* goods, content, or services provided by a *Relying Party*.

## 4 Age assurance process

- 4.1 This document is intended to enable organizations to provide and control access to their services to suitable age-groups, taking into consideration the rights and needs of minors by addressing these processes in sequence:
- a. Compliance and risk assessment (Section 5)
  - b. Selection of *age assurance* method (Section 6)
  - c. Design of *age assurance* technology (Section 7)
  - d. Undertake *age assurance* (Section 8)

## 5 Compliance and risk assessment

- 5.1 The *Relying Party shall*, before designing, developing or deploying an *age assurance* technology, conduct a comprehensive privacy impact assessment to identify privacy risks to individuals that could result from each *age assurance* method contemplated, consider the concept of proportionality and *shall* identify effective measures to avoid, minimize, or mitigate identified risks. This assessment *shall* be periodically updated.
- 5.2 The *Relying Party shall* assess the potential effects of its services or products on minors' rights by conducting a Child Rights Impact Assessment (CRIA)<sup>1</sup>. This includes documentation of how it considers children's rights and best interests in alignment with relevant international human rights obligations, the United Nations Convention on the Rights of the Child (CRC), UNICEF's Child Rights Impact Assessment, Canadian legislation, and policies and practices in the context of minor protection.

NOTE: The Child Rights Impact Assessment Toolbox guides businesses on conducting robust child rights impact assessments in relation to the digital environment. It is intended for use by all companies that are developing, deploying or using digital technologies including Artificial Intelligence.

---

<sup>1</sup> <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA>

- 5.3 The best interests of minors *shall* be a primary consideration in any compliance or risk assessment using an evidence-based approach. Where conflicts of interests between a minor's best interests and other stakeholders emerge, the best interests of the minor *shall* be a primary consideration. Any instances where the best interests of minor were overridden *should* be documented in detail.
- 5.4 The *Relying Party shall* ascertain which jurisdictional privacy and age-based laws and regulations it must comply with (i.e., federal, provincial/territorial and/or municipal/local). This includes where its services or products are offered, and from where *users* are accepted in which *age assurance* plays a part.
- 5.5 The *Relying Party shall* document how it complies with the federal, provincial/territorial, municipal/local requirements and other applicable foreign laws for *age assurance* relevant to each of these jurisdictions, which may include any applicable Canadian online safety legislation.
- NOTE: These requirements may differ based on the types of access provided to different types of goods, content or services, e.g. service-specific minimum age requirements can be different for different Canadian provinces.
- 5.6 The *Relying Party shall* assess the level of risk that its services, or parts of its services, pose for minors of each age or age range and *shall* mitigate against identified risks.
- 5.7 Evaluation of proportionality will include evaluation of the proposed *age assurance* technology using criteria such as sensitivity and necessity, proportionality, effectiveness, and minimal intrusion.

## 6 Selection of age assurance method

- 6.1 The *Relying Party shall* assess the age or age range of the *users* they are engaging with.
- 6.2 The *Relying Party shall* select the age-appropriate method or methods of *age assurance*, based on the level of confidence required for *age assurance* and the proportionality principle, based on the level of risk that the performed risk assessment indicates the technology could present to the user, to ensure the following factors are considered:
- a. Protection of *users' personal information* explicitly prohibiting profiling, repurposing, or secondary use of data
  - b. Accuracy of *age assurance*
  - c. Reliability of *age assurance* method, referring to how consistent the results can be generated and independently verified, and other error detection metrics
  - d. Overall *robustness* of the *age assurance* method

- 6.3 The levels of *age assurance shall* comply with corresponding laws for corresponding services in municipal, provincial and national levels.
- 6.4 The *Relying Party shall* assess and document the minimum level of *Personal information* required to achieve *age assurance* to the level of confidence required.
- 6.5 The *Relying Party* in collecting *Personal information should* account for the principles of minimization, no secondary uses (especially for commercial or other profiling purposes), and timely deletion.
- 6.6 The *Relying Party should* offer multiple options for *age assurance* that provide *users* with effective alternatives taking the context in which *age assurance* is required into account.
- 6.7 The *Age Assurance Provider shall* offer a dispute resolution mechanism to resolve incidents where a *user* states that the *age verification* technology is not accurate.

## **7 Design of age assurance technology**

- 7.1 *Age assurance* technology *shall* be designed, developed and deployed based on the tenets of *Privacy by Design, Privacy by Default, Security by Design*, and proportionality and *data minimization* principles.
- 7.2 *Age assurance* technology *shall* be designed to be transparent, accountable and respectful of the rights and bests interests of individuals, including members of vulnerable populations.  
  
NOTE: The technology *should* not unduly restrict *user* access to materials which they *should* reasonably be able to access, example health and educational materials.
- 7.3 *Age assurance* technology *should* be designed to support interoperability, where a suitable mechanism is available so that the results of an *age assurance* process can be exchanged securely with another *Age Assurance Provider*.
- 7.4 The *Age Assurance Provider* and *Relying Party shall* ensure that the *age assurance* technology is accessible to *users* within defined jurisdictions. The Responsible Authority *shall* document their conformity claims with an appropriate accessibility standard within defined jurisdictions.

NOTE: *Age assurance* technology needs to both be inclusive, to those with disabilities, as well as readily available so all persons in the jurisdiction can access it.

- 7.5 The *Age Assurance Provider shall* issue upon request an *age assurance* statement which summarizes the approach and justification for all design requirements.

## 8 Undertake age assurance

- 8.1 The *Relying Party* shall take appropriate and proportionate measures to ensure assurance of the age or age range of each *user* for *age-restricted* services.

NOTE: The *age assurance* process must be an enabler, not a blocking method. In this way, minors are not subjected to personal data processing and there is no risk that they will be identified, located or targeted. This is particularly important in the context of services that may have both restricted and non-restricted information, such as social media services.

- 8.2 A *Relying Party* shall ensure that, where it has not obtained confirmation that the *user* is above the age threshold for a given feature or item of content, that the *user* is not able to access *age-restricted* content on its products or services. The functionality offered *should* be appropriate to the capacity and age of a potential *user*.
- 8.3 The *Relying Party* shall provide clear, easily understood, and readily available notice to *users* when/if artificial intelligence systems are used at any point in the *age assurance* process.
- 8.4 Each *user* shall be provided with the right, and an effective, direct, and cost-free process by which they can challenge the *Age Assurance Provider's* determination.
- 8.5 The *Age Assurance Provider* shall collect as little *personal information* as necessary for *age assurance* purposes.
- 8.6 The *Age Assurance Provider* should use *personal information* obtained and processed for *age assurance* purposes, solely for *age assurance*.
- 8.7 The *Age Assurance Provider* should not sell, reveal, provide access to, or otherwise divulge or monetize *personal information* obtained and processed for *age assurance* purposes either themselves or to data brokers or other third parties.
- 8.8 The *Age Assurance Provider* shall ensure that all *personal information* used during *age assurance* is stored securely and, unless required by law, is deleted or destroyed as soon as *age assurance* processes are complete, or there is no longer a valid business or legal need to retain the information, whichever is soonest.
- 8.9 If the *Age Assurance Provider* is required by law or lawful demand to retain any of the *personal information* collected for the purpose of *age verification*, for use beyond *age assurance* purposes, the *Age Assurance Provider* shall, unless prohibited by law or lawful process, immediately provide the individual about whom the *personal information* relates with clear justification or rationale for retaining the *personal information* and the secondary purpose(s) for which the *personal information* is being retained.
- 8.10 Excepting the specific individuals authorized by a *Relying Party* to carry out *age assurance* on its behalf, *Relying Parties* should not be able to receive *personal information* about users for whom

they are conducting an *age assurance* process, and *Age Assurance Providers shall* not record which specific identified person is requesting access to a specific *Relying Party*.

## Bibliography

- [1] Australian Senate, *Sexualisation of Children in the Contemporary Media*, Standing Committee on Environment, Communications and the Arts, June 2008.
- [2] *Bill S-210 An Act to Restrict Young Persons Online Access to Sexually Explicit Material*, November 2021.
- [3] Centre for Media, Technology and Democracy, *Youth Assembly on Digital Rights and Safety: 2023*, September 2023.
- [4] Digital Futures Commission and 5Rights Foundation, *Child Rights by Design*, March 2023.
- [5] Emily Laidlaw, *Online Age Verification is Crucial and Bill S-210 Gets It Wrong*, February 2024.
- [6] Government of Canada, *Child Rights Impact Assessment*, July 2023.
- [7] House of Commons, *Ensuring the Protection of Privacy and Reputation on Platforms Such as Pornhub*, Report of the Standing Committee on Access to Information, Privacy and Ethics, June 2021.
- [8] IEEE Standards Association P2089.1, *Standard for Online Age Verification*, 2023.
- [9] ISO/IEC 27566-1, *Information security, cybersecurity and privacy protection – Age assurance systems – Part 1 – Framework*, 2025.
- [10] Kayee Hanaoka, Mei Ngan, Joyce Yang, George W. Quinn, Austin Hom, Patrick Grother (2024) *Face Analysis Technology Evaluation: Age Estimation and Verification*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8525.  
<https://doi.org/10.6028/NIST.IR.8525>
- [11] Office of the Privacy Commissioner of Canada, *Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada*, October 2022.
- [12] Statistics Canada, *Police-reported online child sexual exploitation in Canada, 2022*, March 2024.
- [13] UN General Assembly, *Convention on the Rights of the Child*, United Nations, Treaty Series, vol. 1577, p. 3, 20 November 1989.