CAN/DGSI 120:202X
NATIONAL STANDARD OF CANADA

Edition 2
202X-XX

Use of biometrics for authentication

35.020, 35.240, 35.240.15

WARNING

This document is not an official DGSI Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as a National Standard of Canada.

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.

- Page left intentionally blank -

Table of Contents

- Page left intentionally blank -

Foreword

Digital Governance Standards Institute (DGSI) is a not-for-profit corporation providing a national forum for public and private sector members to transform, shape and influence the Canadian information and technology ecosystem.

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 Council
500-1000 Innovation Drive,
Ottawa, ON K2K 3E7
info@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.

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.

- Page left intentionally blank -

Introduction

This is the Second Edition of CAN/DGSI 120:202X, Use of biometrics for authentication.

CAN/DGSI 120:202X was prepared by the DGSI Technical Committee 15 (TC 15) on Biometrics, comprised of over XX thought leaders and experts in cybersecurity of devices and systems. This Standard was approved by a Technical Committee formed balloting group, comprised of X producers, X government / regulator / policymakers, X users, and X 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 one year 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 technology agnostic.

This Standard is intended to be used for conformity assessment.

ICS 35.020, 35.240, 35.240.15

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

- Page left intentionally blank -

Context

Biometrics can be used for good, resulting in more efficient access to products and services but unfortunately can also be used for fraudulent and corrupt purposes. Furthermore, biometrics technologies have advanced faster than laws and regulations that should address acceptable use with relevant laws to protect against its misuse.

Biometrics technologies are tools that can be used for person verification, authentication, identification, and location. The tools are used by government, industry, consumers for a variety of purposes. However, their use is not without controversy such as its use for surveillance and control of citizens to its unauthorized collection and use for profit. Furthermore, biometrics can be and in many cases is invisible to the average person.

Identity is fundamental to how people conduct their affairs both physically and increasingly digitally. Biometrics can be advantageous for identity verification and authentication. However, its use is not regulated and there is a lack of guidance on how, when and who can use biometrics, for what purpose and how to protect the privacy and security of biometric information.

How can you be sure of someone's identity online? If an individual isn't physically in front of you holding a driver's license or other ID document, how can you be sure that they are who they claim to be? Or that they even exist? The implications of not knowing if someone is genuinely present online can be severe for consumers, businesses, governments, and society as a whole.

Biometric matching is used to verify the identity of individuals in many different applications. Recently, more of these applications occur remotely, where the individual being verified is not present at the point of verification. In these cases, the remote biometric matching needs to be verification to ensure that the biometric collected is a live sample from a real person and that the match result or comparison score is from a trusted source.

Biometric authentication uses computer science to verify those human metrics as a form of identification and access control. The challenge of authentication is letting the right people in while keeping the wrong people out. If authentication is too secure, genuine customers and users may be prevented from accessing an organization's services, their accounts, or their money. If authentication is not secure enough, fraudsters will steal access to services, their accounts, and their money.

The simplicity of biometrics is one if its greatest advantages, anyone can use it. There is no password to remember, and there is no device or access token to carry around. This makes biometrics the most inclusive and accessible method of security there is, if implemented properly. This standard provides practice guidance on biometric authentication, explains various attacks on remote biometric systems and how they can be mitigated to protect customers and organizations.

1 Scope

This document defines minimum requirements for the use of biometrics.

2. Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes the 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.

CAN/DGSI 103-1, Digital Trust and Identity – Part 1: Fundamentals
ISO/IEC 24760, IT Security and Privacy — A framework for identity management - Part 1: Terminology and concepts

3. Terms and Definitions

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

authentication
A process that verifies the legitimacy of a biometric that links the privilege holder with the claimant trying to obtain the privilege.

authenticator
Something that a holder controls (something they own, something they know, or something they are such is biometrics) that is used to demonstrate that the holder retains control of a credential.

[SOURCE: CAN/DGSI 103-1:2023 Digital Trust and Identity - Part 1: Fundamentals]

biometric binding
Binding of the vetted claimed identity to the individual through biometrics according to the issuing authority.

biometric template
A mathematical representation of biometric features extracted from a biological sample. Templates are typically irreversible and cannot be reconstructed into the original biometric image. Templates are algorithm-specific and generally not interoperable across systems.

contextual or functional identity
Evidence of Identity, which establishes the existence or digital representations of entities within a particular context and for a specified purpose after Foundational Evidence of Identity has been proven and accepted.

detection/deduplication
Biometric identification is used to identify potential duplications between applicants for enrolment and previously verified and enrolled profiles in a database.

foundational evidence of identity
Evidence of Identity that establishes the existence, uniqueness, and Digital Representation of real, legally recognized Identities, based on fact-based foundational events (e.g., birth, immigration, incorporation). The establishment and maintenance of foundational identity evidence is the exclusive domain of the public sector.

identification
The process of establishing the identity of an unknown person by establishing a connection between unknown and unverified data and known and verified data.

identity
A reference or designation used to uniquely distinguish a particular Person, organization, or device.

[SOURCE: CAN/DGSI 103-1:2023 Digital Trust and Identity - Part 1: Fundamentals]

identity proofing
A process of establishing a level of confidence with respect to the Foundational or Functional (Conceptual Identity) of an applicant through validation and verification during enrollment in an Identity Management System (IdMS).

liveness detection
Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions in order to determine whether a biometric sample is being captured from a living subject present at the point of capture

NOTE: Liveness detection methods are a subset of presentation attack detection methods.

[SOURCE:ISO/IEC 30107-1:2023, Information technology — Biometric presentation attack detection - Part 1: Framework]

presentation attack
Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

NOTE 1: Biometric presentation attacks can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc.

NOTE 2: Biometric presentation attacks can have a number of goals, e.g. impersonation or not being recognized.

NOTE 3: Biometric systems can be unable to differentiate between presentations with the goal of interfering with the systems' operation and non-conformant presentations.

[SOURCE:ISO/IEC 30107-1:2023, Information technology — Biometric presentation attack detection Part 1: Framework]

trust Framework
A set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approaches.

[SOURCE: CAN/DGSI 103-1:2023 Digital Trust and Identity Part 1: Fundamentals]

validation
This is a process to authenticate or legitimize Personal Identifiers (or Identity Attributes) presented by applicants during enrollment in an Identity Management System.

verification
Provable high confidence in the claimed connection between applicant and validated Personal Identifiers or Identity Attributes.

4. Principles of Biometric Use

4.1 Biometrics shall only be used where it is necessary to meet a specific need and where the loss of privacy is proportionate to privacy laws compared to the benefits gained.

4.2 Biometric technology shall be accurate, minimize data collection, limit personal information collection to that required to fulfill a specific purpose and keep biometric information only for the purpose stated.

4.3 Biometric technology used shall consider accessibility, equitability and the needs of vulnerable persons.

4.4 Evaluation of proportionality should include evaluation of the proposed biometric program's scope using criteria such as sensitivity and necessity, proportionality, effectiveness, minimal intrusiveness, and minimal intrusion.

5. Biometric Collection Disclosure

5.1 Each collection, management, and use of biometric data shall specify the purpose and the goal with details on how the purpose is specifically achieved with the use of the biometric information.

5.2 This statement shall acknowledge legal obligations regarding its collection, use and disclosure.

5.3 These statements should be disclosed in a single and broader Notice of Privacy Policy.

5.4 Disclosures to relevant persons shall be directed specifically to them.

6. Biometric Privacy and Security Risk Disclosure

6.1 Biometrics-using organizations shall be responsible for the encryption and protection of biometric and personal data they collect and process.

6.2 Biometrics-using organizations shall implement security safeguards appropriate for the information's sensitivity and risk.

6.3 Biometric data shall be protected because of the potential harm from breaches of private information or biometrics.

6.4 Institutions and organizations that use biometrics to protect personal data shall establish appropriate safeguards against spoofing, falsification, attack methods, vulnerability assessments, and testing.

6.5 Institutions and organizations using biometric systems shall undergo a comprehensive Privacy Impact Assessment (PIA), particularly in cases where personal and biometric data are collected, processed, or transmitted remotely.

NOTE: Need a suggested reference to a PIA.

6.6 A Biometric Privacy Risk Disclosure shall describe and make it easy for ordinary consumers to understand the risk and responsibility associated with the collection, management or use of biometric information.

6.7 These statements shall be disclosed in a single and broader Notice of Privacy Policy.

6.8 All relevant persons should be directed to such disclosures.

6.9 When using biometric templates, institutions and organizations shall ensure that templates are encrypted.

NOTE: Encryption applies to templates when the organization stores or controls them. Many architectures (e.g., match-on-device systems) never expose templates at all, so the requirement cannot apply universally.

6.10 Encrypted templates shall be stored separately from encryption keys.

7. Voluntary Consent to Biometric Data Collection and Use

7.1 Individuals shall acknowledge that they have read and understood the Statement of Biometric Use and Collection, as well the Biometric Privacy Risk Disclosure.

7.2 Before any biometric data collection can take place, all individuals shall either consent or decline to it.

7.3 If there is a valid exception to the consent requirement, any extension of the biometrics use shall be obtained from the individual. Subject to contractual or legal restrictions, individuals have the right to withdraw consent that they have previously given.

7.4 If required by law, individuals shall be given an easy and simple way to withdraw their consent.

8. Compliance and Audit Use

8.1 Any management or use of biometric data shall ensure that there is clear legal authority to collect and use biometrics for the stated purpose. They also need to comply with the Statement of Biometric Use.

8.2 Only the consented-to and specifically described use of data collected will be allowed.

8.3 All data usage shall be recorded, audited periodically, and made readily available for review upon request.

8.4 Any violation of this compliance, reasonable effort shall be made to report as soon as possible to the individual concerned and all other stakeholders, including the relevant government regulatory bodies and law enforcement.

8.5 Biometric systems shall maintain audit trails verifying enrollment, authentication attempts, re-verifications, and template management events.

8.6 Institutions and organizations using biometrics shall implement secure deletion protocols.

9. Identity Verification and Enrolment Process

9.1 Identity Verification is a foundational prerequisite for any biometric authentication system. Before biometrics can be used to authenticate individuals, it shall be confirmed that the biometric sample being registered belongs to a verified person.

9.2 The biometric authentication system enrollment process shall:

a. Establish a unique and verifiable identity based on foundational or contextual identity evidence.

b. Ensure that the biometric sample is collected from a live person present during the session (e.g., using liveness detection or in person enrollment).
c. Prevent duplicates by performing deduplication against known identity databases.

NOTE: Deduplication generally requires access to raw images. Systems with encrypted or device-bound templates cannot technically perform deduplication.

9.3 Identity Proofing during biometric authentication system enrollment shall include:

a. Validation of personal identifiers (e.g., name, date of birth, government-issued ID).
b. Verification of the claimed identity through trusted sources (e.g., passport office, driver's license registry).

9.4 Biometric authentication system enrollment should use public key cryptography (PKC). A unique private key should be cryptographically bound to the biometric credential.

9.5 Biometric authentication system enrollment procedures shall be logged and subject to audit. A record of the identity proofing and biometric binding shall be maintained in a secure and privacy-preserving manner.

9.6 All identity verification and enrollment processes shall comply with applicable privacy legislation and should follow best practices outlined in national and international identity standards (e.g., CAN/DGSI 103-1, ISO/IEC 24760).

9.7 If a credential is lost or compromised the institution or organization shall refer to CAN/DGSI 103-1, Digital Trust and Identity – Part 1: Fundamentals, for the purposes of recovery or revocation procedures.

10. Strong Authentication Using Biometric Binding

10.1 Biometrics combined with Public Key Cryptography (PKC) systems can achieve strong authentication by combining biometrics ("something you are") with hardware-backed secure device possession ("something you have").

NOTE: More information is available in Annex A: Credential Authentication in Detail

10.2 Institutions and organizations using biometrics for strong authentication shall implement the following security measures:

- Non-exportable private keys.
- Local-only encrypted biometric template storage.
- Passwordless authentication.
- Audit traceability.

10.3 Institutions and organizations using biometrics shall implement the following technical setup elements:

- One-time enrollment with a refresh capability (ID + biometric + key generation).
- Challenge-based live authentication against biometric templates that release the private key (biometric match + cryptographic signing).

NOTE: The rigor of the requirements for the initial enrollment process should be maintained when performing a refresh.

10.4 Biometric templates created during remote identity proofing via live biometrics and government ID should be digitally signed by the identity proofing authority and stored alongside the public key in a PKC system. Such collections shall be recognized as the collection of Personally Identifiable Information (PII) and require explicit acceptance and consent from the individual. The benefit to the individual includes enhanced security because templates can be randomly verified, further protecting against identity theft and providing a method for continuous authentication and integrity assurance.

Annex A: Credential Authentication in Detail

(Informative)

Credential authentication is the process of verifying that a Holder has control over an issued Credential. Control of an issued Credential is verified by means of one or more authenticators.

NOTE: The degree of control over the issued Credential can be used to generate a level of assurance.

A.1 Authenticators

An authenticator is something that a Holder controls that is used to prove that the Holder has retained control over an issued Credential. There are three types of authenticators:

- Something the Holder owns and controls (e.g., a cryptographic hardware key, a phone, a computer, etc.). Caution must be exercised because someone can impersonate the Holder by taking control of their device. The fraudulent re-registration of a Subscriber Identity Module (SIM) or "SIM Swap" is an example of how a device can be stolen "virtually" from the proper Holder. Ownership authentication should be used in conjunction with one of the other authentication methods, ideally biometric authentication.
- Something the Holder knows (e.g., a password, a response to a challenge question, a one-time-password). The exclusive use of secrets such as passwords should be treated with extreme caution since passwords can be stolen by means of a wide array of methods and as a result, passwords can be changed without the Holder's or Issuer's knowledge or involvement. As a rule, knowledge-based authentication should only be used in conjunction with one of the other authentication methods.
- Something the Holder is or does, i.e., the Holder's biometrics (e.g., face, fingerprints, retinas, keyboard stroke timing, gait). The use of a biometric authenticator should incorporate liveness and similar presentation attack defenses to prevent spoofing of the biometric. Biometric authentication should be used in conjunction with one of the other authentication methods, ideally ownership authentication. This is because biometric authentication should require the active knowledge and/or involvement of the Holder and is therefore dependent on the Holder's active control of the device which processes the biometrics.

It should be noted that the irrevocability of biological characteristics (e.g., face, fingerprints, retinas) makes the use of biometric authentication attractive for Credential Verification. A Holder's biological characteristic cannot be easily changed. Nor can a Holder's biological characteristic be easily replicated; nonetheless, industry standards include requirements for robust liveness detection and similar anti-spoofing techniques to protect against biometric replication attempts.

However, industry standards are generally cautious in regards to the exclusive use of biological characteristics as authenticators for Credentials. Biometric authentication should be used in conjunction with ownership authentication.

Bibliography

[1] Biometric Authentication for Dummies (2022). iProov Special Edition, John Wiley and Sons Limited, Chichester, West Sussex, United Kingdom.

[2] CAN/DGSI 103-1, Digital Trust and Identity – Part 1: Fundamentals

[3] Guidance on the Acceptable Use of Biometrics (2020). Digital ID and Authentication Council of Canada (DIACC), Toronto, ON.

[4] ISO/IEC 24760, IT Security and Privacy — A framework for identity management - Part 1: Terminology and concepts