National Standard of Canada
Standards Proposal

Proposed Standard Title:

Guidance for Authentication of Remote Biometrics

Plain Language Summary of Standards Proposal (200 words max):

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 authenticated 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.

This standard proposes to explain various attacks on remote biometric systems and how they can be mitigated. Depending on the types of mitigation and which attacks they cover, an authentication score can be computed. Trust can be assigned to the remote biometric process for different types of applications depending on its authentication score.

Proposed Scope:

This proposed standard will define the minimum requirements of remote identity verification using biometrics. It will also list various attack types and explain how they can subvert the biometric verification process. Then it will define methods that can be used to detect or invalidate the attacks, allowing the biometric verification to be authenticated remotely.

Authentication methods which have not yet been devised can also reference this standard if they can demonstrate how they detect or invalidate the various attack types.

Strategic Need:

Identify the strategic need of key stakeholders and confirmation expressing the need.

This includes consideration for:

- a. *The strategic need of key stakeholder (e.g. legislator, industry, government, consumers);*
- b. *The type of standard (international, regional, domestic standards and harmonization need);*
- c. *Addressing up-to-date vs outdated standard to ensure latest innovative/technology/safety features available for businesses;*
- d. *If the standard is intended to support national/regional/international certification programs;*
- e. *If there is stakeholder intention to transition to different standard;*
- f. *The type of maintenance (periodic, continuous, stabilized, best before date); and*
- g. *The use of "CAN" descriptor.*

The use of biometric matching to verify identity has become ubiquitous in recent years. From its early association with latent fingerprint matching as part of criminal investigations, biometric technology has advanced to be used as part of border crossings, financial transactions, and even unlocking mobile devices. Over time, more of these applications have come to rely on remote biometric matching where the individual identifies themselves without any visit to a commercial or government site. Since the start of the COVID-19 pandemic, the desire for remote biometrics has accelerated as government and businesses figure out how to engage with individuals without requiring in-person interactions. In many cases remote biometrics are now being used to onboard individuals into new systems and not just for individual transactions within existing systems. In these cases, the chain of trust for the entire system is dependent upon the validity of the initial remote biometric transaction.

Companies and governments that deploy these remote biometric systems are often unfamiliar with the specific security issues surrounding their use. Standards already exist to address biometric quality [1], the measurement of biometric performance [2] and even the issue of spoofing (also known as a presentation attack) [3]. There is also useful guidance information in the ISO technical Report on biometrics for mobile devices [4] and especially in the FIDO Alliance Biometrics Requirements [5]. All of these documents are very helpful to mobile device manufacturers and for entities deploying biometric matching technology on mobile devices. There are even certification programs for mobile devices that ensure a minimum accuracy for biometric matching and minimum levels of protection against presentation attacks.

What is lacking is an overall standard that explains the specific issues of remote biometric matching and how the different components such as biometric matching accuracy, presentation attack detection, injection attack detection, geolocation, video monitoring and other techniques can be combined to provide authentication of the remote biometric matching process with different levels of security that are suitable for different applications. All entities deploying remote biometrics would benefit from such guidance because it would make it possible for them to match the security techniques deployed around mobile authentication to the security profile of the particular application using the remote biometrics. Requiring too much security for every application is costly and less convenient for end users, but requiring too little security brings significant risks.

Need for Availability in Both of Canada's Official Languages: *Do stakeholders need the standard published in both official languages?* *Do users of the standard need the standard published in both official languages?* *Do authorities having jurisdiction need the standard published in both official languages?* *Are there health and safety related needs for the standard to be published in both official languages?* *For adoptions, is there availability of the regional/international standard or other deliverable from the source?* *For adoptions, is there an agreement with the source committee to facilitate official translation?*	Y

Geographical Representation Considerations:

Identify the Canadian geographical representation appropriate to the subject area covered by the standard.

Geographic representation may consider factors such as:

a. Industry (e.g. petroleum in petroleum producing provinces);

b. Reference in regulation (if a regulation exists in a province); or

c. Commodity characteristics and social impact (e.g. heating oil for northern climates).

The proposed standard spans all sectors/domains and is Canada wide.

Trade:

Identify how the standard meets the needs of the marketplace and contributes to advancing trade in the broadest possible geographical and economic contexts.

For example:

a. Facilitate Canadian innovation to lead internationally;

b. Support the objectives of "One standard, one test, accepted everywhere";

c. Support the objectives of "First to Market"; or

d. Foster international/ regional/ national alignment of requirements.

Developing the proposed standard would provide guidance that would simplify decision making during the deployment of new systems and applications using remote biometrics. It would enable Canadian companies to take advantage of existing standards and certification programs in the field of mobile biometrics but would also allow informed decisions to be made about balancing security with the requirements of the application. This would simplify deployment and help to avoid both increased cost due to excessive security and increased risk due to insufficient security. The net result should be an increase in the number of successful projects using remote biometrics within Canada and for Canadian companies to capture a larger part of this growing market internationally.

Relevant existing documents at the international, regional and national level:

[1] ISO/IEC 29794-1:2016 Information technology — Biometric sample quality – Multi-part standard

[2] ISO/IEC 19795-1:2021 Information technology — Biometric performance testing and reporting – Multi-part standard

[3] ISO/IEC 30107-1 Information technology — Biometric presentation attack detection — Multi-part standard

[4] ISO/IEC TR 30125:2016 Information technology — Biometrics used with mobile devices

[5] FIDO Biometrics Requirements – FIDO Alliance, December 06, 2021