



Norme nationale du Canada Proposition de normes

Titre proposé de la norme :

Conseils pour l'authentification à distance de la biométrie

Résumé en langage clair de la proposition de normes (200 mots maximum) :

La mise en correspondance biométrique est utilisée pour vérifier l'identité des individus dans de nombreuses applications différentes. Récemment, un plus grand nombre de ces applications ont lieu à distance, la personne faisant l'objet de la vérification n'étant pas présente au point de vérification. Dans ces cas, la mise en correspondance biométrique à distance doit être authentifiée pour veiller à ce que l'information biométrique recueillie représente un échantillon vivant d'une personne réelle et à ce que le résultat de la correspondance ou le score de comparaison provienne d'une source fiable.

Cette norme propose d'expliquer diverses attaques sur les systèmes biométriques distants et la manière dont le risque peut être atténué. Selon les types de mesures d'atténuation et les attaques qui sont couverts, un score d'authentification peut être calculé. On peut faire confiance au processus biométrique à distance pour différents types d'applications en fonction de son score d'authentification.

Portée proposée :

Cette norme proposée définira les exigences minimales de la vérification d'identité à distance à l'aide de la biométrie. Elle répertoriera également divers types d'attaques et expliquera de quelles façons ceux-ci peuvent subvertir le processus de vérification biométrique. Ensuite, elle définira des méthodes permettant de détecter ou de neutraliser les attaques pour permettre l'authentification à distance de la vérification biométrique.

Les méthodes d'authentification qui n'ont pas encore été conçues peuvent également faire référence à cette norme si elles peuvent démontrer de quelle manière elles détectent ou neutralisent les différents types d'attaques.

Besoin stratégique :

Déterminer le besoin stratégique des parties prenantes clés et obtenir une confirmation qui exprime ce besoin.

Les facteurs suivants seront pris en compte :

- a. *Le besoin stratégique de la partie prenante principale (p. ex., le législateur, le secteur, le gouvernement, les consommateurs);*
- b. *Le type de norme (norme internationale, régionale ou nationale et le besoin d'harmonisation) ;*
- c. *La reconnaissance des normes à jour par rapport aux normes désuètes pour s'assurer que les entreprises aient accès aux plus récentes caractéristiques en matière d'innovation, de technologie et de sécurité ;*
- d. *Le soutien aux programmes de certification nationaux, régionaux ou internationaux comme objectif de la norme ;*
- e. *L'existence d'une volonté des parties prenantes de passer à une norme différente ;*

f. *Le type de maintenance (périodique, continue, stabilisée, à durabilité minimale) ;
L'utilisation d'un descripteur « CAN ».*

L'utilisation de la mise en correspondance biométrique pour vérifier l'identité est devenue omniprésente ces dernières années. Depuis son association précoce avec la correspondance d'empreintes digitales latentes dans le cadre d'enquêtes criminelles, la technologie biométrique a évolué pour être utilisée dans le cadre de mouvements transfrontaliers, de transactions financières et même du déverrouillage d'appareils mobiles. Au fil du temps, un plus grand nombre de ces applications en sont venues à s'appuyer sur la mise en correspondance biométrique à distance dans le cadre de laquelle l'individu s'identifie sans se rendre à un emplacement commercial ou gouvernemental. Depuis le début de la pandémie de COVID-19, l'attrait de la biométrie à distance s'est accru à mesure que le gouvernement et les entreprises découvrent comment interagir avec les individus sans que des interactions en personne soient nécessaires. Dans de nombreux cas, la biométrie à distance est désormais utilisée pour intégrer des individus dans de nouveaux systèmes et pas seulement pour des transactions individuelles au sein de systèmes existants. Dans ces cas, la chaîne de confiance pour l'ensemble du système dépend de la validité de la transaction biométrique à distance initiale.

Les entreprises et les gouvernements qui déploient ces systèmes biométriques à distance ne connaissent souvent pas les problèmes de sécurité particuliers liés à leur utilisation. Des normes existent déjà pour traiter de la qualité biométrique [1], de la mesure de la performance biométrique [2] ou encore de la question de la mystification (également appelée incitation à la faute) [3]. Il existe également des informations pratiques utiles dans le Rapport technique de l'ISO sur la biométrie pour les appareils mobiles [4] et en particulier dans les Exigences biométriques de l'Alliance FIDO [5]. Tous ces documents sont très utiles aux fabricants d'appareils mobiles et aux entités déployant la technologie de mise en correspondance biométrique sur les appareils mobiles. Il existe même des programmes de certification pour les appareils mobiles qui garantissent une précision minimale pour la correspondance biométrique et des niveaux minimaux de protection contre les attaques par mystification.

Ce qui manque, c'est une norme globale qui explique les problèmes particuliers de la mise en correspondance biométrique à distance ainsi que la façon dont les différents composants tels que la précision de la mise en correspondance biométrique, la détection des attaques par mystification, la détection des attaques par injection, la géolocalisation, la surveillance vidéo et d'autres techniques peuvent être combinés pour authentifier le processus de mise en correspondance biométrique à distance avec différents niveaux de sécurité adaptés à différentes applications. Toutes les entités déployant la biométrie à distance bénéficieraient de ces conseils, car cela leur permettrait d'adapter les techniques de sécurité déployées dans le cadre de l'authentification mobile au profil de sécurité de l'application particulière utilisant la biométrie à distance. Exiger trop de sécurité pour chaque application est coûteux et moins



pratique pour les utilisateurs finaux, mais exiger trop peu de sécurité comporte des risques importants.

Besoin de disponibilité dans les deux langues officielles du Canada :

*Les parties prenantes jugent-elles nécessaire que la norme soit publiée dans les deux langues officielles ?
Les utilisateurs de la norme jugent-ils nécessaire que celle-ci soit publiée dans les deux langues officielles ?
Les autorités compétentes jugent-elles nécessaire que la norme soit publiée dans les deux langues officielles ?
Est-il nécessaire, sur les plans de la santé et la sécurité, que la norme soit publiée dans les deux langues officielles ?
En ce qui concerne les adoptions, la norme régionale ou internationale (ou tout autre produit livrable) est-elle mise à disposition à partir de la source ?
En ce qui concerne les adoptions, existe-t-il une entente avec le comité de la source pour faciliter une traduction officielle ?*

Oui

Considérations relatives à la représentation géographique :

Indiquez la représentation géographique canadienne qui convient au domaine visé par la norme.

La représentation géographique peut tenir compte de facteurs comme :

- a. L'industrie (p. ex., le pétrole dans les provinces productrices de pétrole) ;
- b. La référence en réglementation (si la province possède une réglementation) ; ou
- c. Les caractéristiques et l'impact social des produits de base (p. ex., le mazout de chauffage pour les climats nordiques).

La norme proposée s'applique à tous les secteurs/domaines et à l'ensemble du Canada.

Commerce :

Indiquez de quelle manière la norme répond aux besoins du marché et contribue à favoriser le commerce dans les contextes géographiques et économiques les plus vastes possible.

Par exemple :

- a. Faciliter l'innovation canadienne afin qu'elle joue un rôle de premier plan à l'échelle internationale ;
- b. Appuyer les objectifs du principe « Une norme, un essai, acceptés partout » ;
- c. Appuyer les objectifs consistant à « Être les premiers à commercialiser » ; ou
- d. Favoriser l'harmonisation des exigences à l'échelle internationale, régionale et nationale.

L'élaboration de la norme proposée fournirait des orientations qui simplifieraient la prise de décision lors du déploiement de nouveaux systèmes et applications utilisant la biométrie à distance. Cela permettrait aux entreprises canadiennes de profiter des normes et des programmes de certification existants dans le domaine de la biométrie mobile, mais permettrait également de prendre des décisions éclairées au sujet de l'équilibre entre la sécurité et les exigences de l'application. Cela simplifierait le déploiement et aiderait à éviter à la fois une augmentation des coûts due à une sécurité excessive et un risque accru dû à une sécurité insuffisante. Le résultat net devrait être une augmentation du nombre de projets fructueux utilisant la biométrie à distance au Canada et permettre aux entreprises



canadiennes de s'emparer d'une plus grande partie de ce marché en pleine expansion à l'échelle internationale.

Documents pertinents existants à l'échelle internationale, régionale et nationale :

- [1] ISO/IEC 29794-1:2016 Technologies de l'information — Qualité d'échantillon biométrique – Norme en plusieurs parties
- [2] ISO/IEC 19795-1:2021 Technologies de l'information — Essais et rapports de performance biométrique – Norme en plusieurs parties
- [3] ISO/IEC 30107-1 Technologies de l'information — Détection d'attaque de présentation en biométrie – Norme en plusieurs parties
- [4] ISO/IEC TR 30125:2016 Technologies de l'information — Biométrie utilisée avec des appareils mobiles
- [5] Exigences biométriques FIDO – Alliance FIDO, 6 décembre 2021