# Biométrie

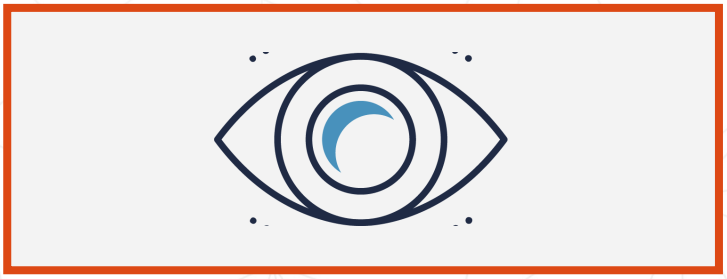
**Février 2024** **ITSAP.00.019**

La biométrique fait référence à la mesure et à l'utilisation des caractères physiques uniques ou des comportements d'une personne, comme les empreintes digitales, la rétine, la structure faciale, la voix, la forme des veines ou la démarche à des fins de sécurité et d'authentification. Si vous recourez à l'authentification biométrique, nous vous recommandons toutefois d'utiliser également des facteurs d'authentification supplémentaires, comme un mot de passe ou un NIP afin d'ajouter une protection supplémentaire. C'est ce que l'on appelle l'authentification multifacteur (AMF). Il faut toutefois savoir que la biométrie apporte son lot d'avantages et d'inconvénients de même que des vulnérabilités qui sont mis de l'avant dans le présent document.

## Comment est saisie la biométrie?

La biométrie peut être saisie de plusieurs manières. Voici des exemples d'appareils de biométrie :

- Les lecteurs d'empreintes digitales permettent de mesurer des courants électriques ou d'émettre des ultrasons qui reproduisent les motifs de vos empreintes digitales;
- Les systèmes de reconnaissance faciale photographient votre visage et comparent la photo prise aux images qui vous correspondent;
- Les systèmes de reconnaissance de l'iris photographient votre œil à l'aide d'une lumière infrarouge et comparent la photo prise aux caractéristiques de votre iris;
- Les systèmes de reconnaissance des réseaux veineux comportant un lecteur émettent une lumière infrarouge afin de créer une image des veines apparaissant dans votre main;
- Les systèmes d'identification du locuteur analysent une combinaison de sonorités de votre voix ainsi que d'autres caractéristiques individuelles (p. ex. votre accent, votre rythme, votre vocabulaire);
- Un système de reconnaissance de la démarche utilise des caméras pour surveiller et analyser vos mouvements (p. ex. vos enjambées et votre cadence) pour vérifier votre identité.



## Quelles sont les utilités associées à la biométrie?

La biométrie s'avère utile pour vous authentifier. En effet, plutôt que d'avoir à entrer un mot de passe ou une phrase de mots, vous pouvez aisément recourir à vos caractéristiques biométriques.

Les organismes peuvent se servir de la biométrie dans différentes circonstances, notamment les suivantes :

- gérer l'accès aux installations d'un édifice, comme les salles de serveurs;
- déverrouiller les actifs et les dispositifs de TI;
- procéder à des paiements à partir de téléphones intelligents.

## Comment puis-je commencer à utiliser la biométrie?

La première fois que vous utilisez la biométrie sur un dispositif, vous devez enregistrer votre caractéristique unique dans le cadre du processus d'inscription. À titre d'exemple, le lecteur d'empreintes procède au balayage de vos empreintes digitales plusieurs fois afin que le dispositif puisse analyser et conserver un code de hachage associé à votre caractéristique biométrique unique. Ce code représente en fait vos empreintes digitales chiffrées et est vraiment difficile à déchiffrer pour les pirates. Un dispositif n'enregistre donc jamais l'image de vos empreintes digitales comme telles.

Avant d'utiliser un système biométrique sur votre dispositif, nous vous recommandons d'effectuer des recherches pour vous assurer que les mécanismes de sécurité du système cadrent avec les exigences de votre organisme.

**SÉRIE SENSIBILISATION**



No de cat. D97-1/00-019-2023F-PDF
ISBN 978-0-660-68192-4

## Quelles sont certaines des menaces associées à la biométrie?

Malgré le caractère unique de vos caractéristiques biométriques, des auteures et auteurs de menace peuvent tout de même les reproduire, les copier ou les imiter afin de déjouer des systèmes. Ils peuvent par exemple faire ce qui suit :

- copier vos empreintes digitales avec des empreintes digitales synthétiques servant de clés maîtresses;
- utiliser une photo tirée de votre profil de médias sociaux pour déjouer un système de reconnaissance faciale;
- obtenir une image de votre iris pour tromper un système de reconnaissance de l'iris en utilisant une image imprimée de votre iris;
- enregistrer ou métamorphoser votre voix pour tromper un système d'identification du locuteur en faisant l'extraction de votre voix pour la superposer sur la voix d'une ou d'un pirate informatique.

Il est à noter que les menaces propres aux médiaux sociaux ne cessent d'augmenter. De fait, grâce à vos comptes de médias sociaux, les auteurs de menace peuvent accéder facilement aux photos et aux vidéos que vous partagez publiquement. N'oubliez donc pas que les éléments que vous publiez peuvent servir à imiter vos caractéristiques biométriques.

## Quels sont certains des problèmes associés aux systèmes biométriques?

Les systèmes biométriques peuvent être défaillants et refuser ou autoriser l'accès à un système ou à un dispositif. Il se produit alors ce que l'on appelle un faux négatif ou un faux positif.

On entend par **faux négatif** les situations où un système biométrique ne reconnaît pas la personne réelle et bloque ses accès. Un cas de faux négatif peut représenter une menace pour votre organisme. En effet, si une infrastructure de serveurs est par exemple hors service et si le personnel autorisé ne peut pas y accéder, votre organisme perd tous ses accès jusqu'à ce que le problème de faux négatif se règle ou qu'une personne réussisse finalement à accéder à l'infrastructure.

En revanche, on entend par **faux positif** les situations où un système biométrique fait correspondre par erreur les justificatifs d'identité de deux personnes différentes. Ainsi, si une personne ne détenant pas d'autorisation se trouve dans une situation de faux positif, votre organisme et la personne détenant les justificatifs d'identité utilisés sont à risque. Par exemple, si votre téléphone intelligent octroie un accès à une personne autre que vous à la suite d'une mauvaise reconnaissance faciale, vos renseignements personnels risquent d'être compromis.

Les faux négatifs et les faux positifs sont possibles. Nous recommandons donc l'utilisation d'un mot de passe ou d'un NIP associée à l'utilisation d'un facteur biométrique afin d'ajouter une protection supplémentaire.

## Quel est le degré de sécurité des nouvelles structures?

Dans la foulée des récents progrès technologiques, on observe l'amélioration des mesures de sécurité protégeant vos caractéristiques biométriques contre les cyberattaques courantes. Les exemples suivants donnent certaines nouvelles caractéristiques et technologies à rechercher à cet effet :

- Les nouveaux systèmes de reconnaissance faciale s'appuient désormais sur des méthodes utilisant des points de lumière infrarouge qui créent un schéma 3D du visage d'une utilisatrice ou d'un utilisateur. Il est peu probable qu'une photo prise sur un compte de médias sociaux donne accès à un dispositif.
- Le balayage des veines de la paume représente une méthode d'authentification biométrique assurant une protection considérable. En effet, les veines ne sont pas aussi facilement visibles que votre visage ou vos empreintes digitales, ce qui complique le vol de votre motif veineux par une personne malveillante.
- Les vérifications du caractère vivant fondées sur le mouvement sont utilisées sur certains dispositifs plus récents pour s'assurer que le balayage est effectué sur une vraie personne.

## Quels enjeux relatifs à la vie privée associe-t-on à la biométrie?

Bien que la biométrie puisse constituer une méthode d'authentification utile, il s'agit également d'une forme de renseignement personnel. Par conséquent, si votre organisme souhaite recourir à la biométrie dans le cadre d'une authentification à facteurs multiples, il doit s'assurer que ce type de données est recueilli, traité et utilisé conformément à des exigences juridiques et réglementaires, comme la *Loi sur la protection des renseignements personnels* (LPRP) et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Les employées et employés doivent également donner leur consentement à l'organisme avant que celui-ci recueille et utilise leurs caractéristiques biométriques.

## Quelles mesures de protection pouvez-vous prendre?

Nous vous recommandons en fait de jumeler l'authentification biométrique à un autre mécanisme d'authentification, comme des phrases de passe. L'authentification à facteurs multiples permet de renforcer le niveau de sécurité. Ainsi, en cas de compromission de l'un des mécanismes d'authentification, l'autre mécanisme utilisé continuera de protéger l'accès à vos dispositifs ou à vos comptes.

Contrairement à d'autres mécanismes d'authentification, comme les mots de passe ou les cartes à puce, il est impossible de deviner ou de voler une caractéristique biométrique. Or, si une caractéristique biométrique particulière comme les empreintes digitales de l'index est imitée ou copiée, il sera impossible d'en obtenir de nouvelles, contrairement à un mot de passe ou à un NIP. Il faudra donc remplacer cette caractéristique biométrique par une autre, comme les empreintes digitales d'un autre doigt ou le balayage de la rétine, pour empêcher des auteures et auteurs de menace d'accéder à des systèmes et à des dispositifs.

## Pour en savoir plus :

Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)

Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)