FINGERPRINTS

UN PAIEMENT EN TOUTE CONFIANCE

MOBILISER LA BIOMÉTRIE POUR LES CARTES DE PAIEMENT

« Il a fallu du temps et un savoir-faire incroyable pour doter les cartes de paiement de capteurs d'empreintes digitales. 2021 et le futur verront les cartes biométriques déployées par les banques et les institutions financières du monde entier, au bénéfice de leur activité, des commerçants et des consommateurs. Les distributeurs doivent comprendre la technologie elle-même pour prendre des décisions éclairées, afin de proposer aux clients une carte qui améliore l'expérience d'achat, au lieu de l'entraver. »

Michel Roig, SVP Business Line Payments & Access à Fingerprints

SOMMAIRE

CHAPITRE 01

01

Biométrique 101

BIOMÉTRIQUE 101

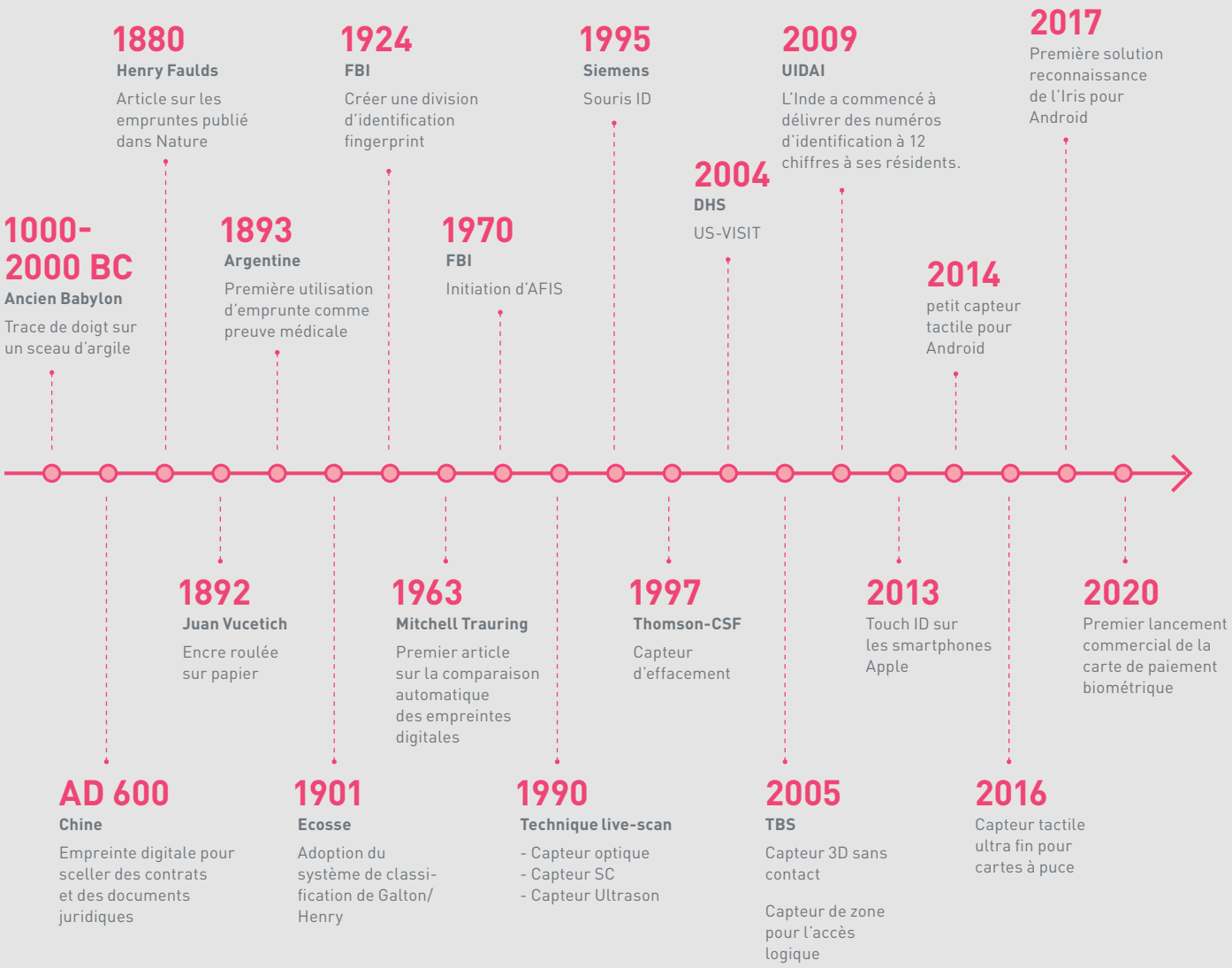
Nous devons constamment prouver qui nous sommes. Il faut ouvrir des serrures, accéder à des appareils et effectuer des achats – Il est essentiel que seules les personnes autorisées puissent effectuer ces tâches. Avec autant d'activités nécessitant une authentification rapide, fiable et pratique, il n'est pas surprenant que la vérification d'identité soit devenue une pierre angulaire de la société actuelle, permettant des interactions sécurisées tout en prévenant la fraude et la criminalité.

BIOMÉTRIE – SON HISTOIRE

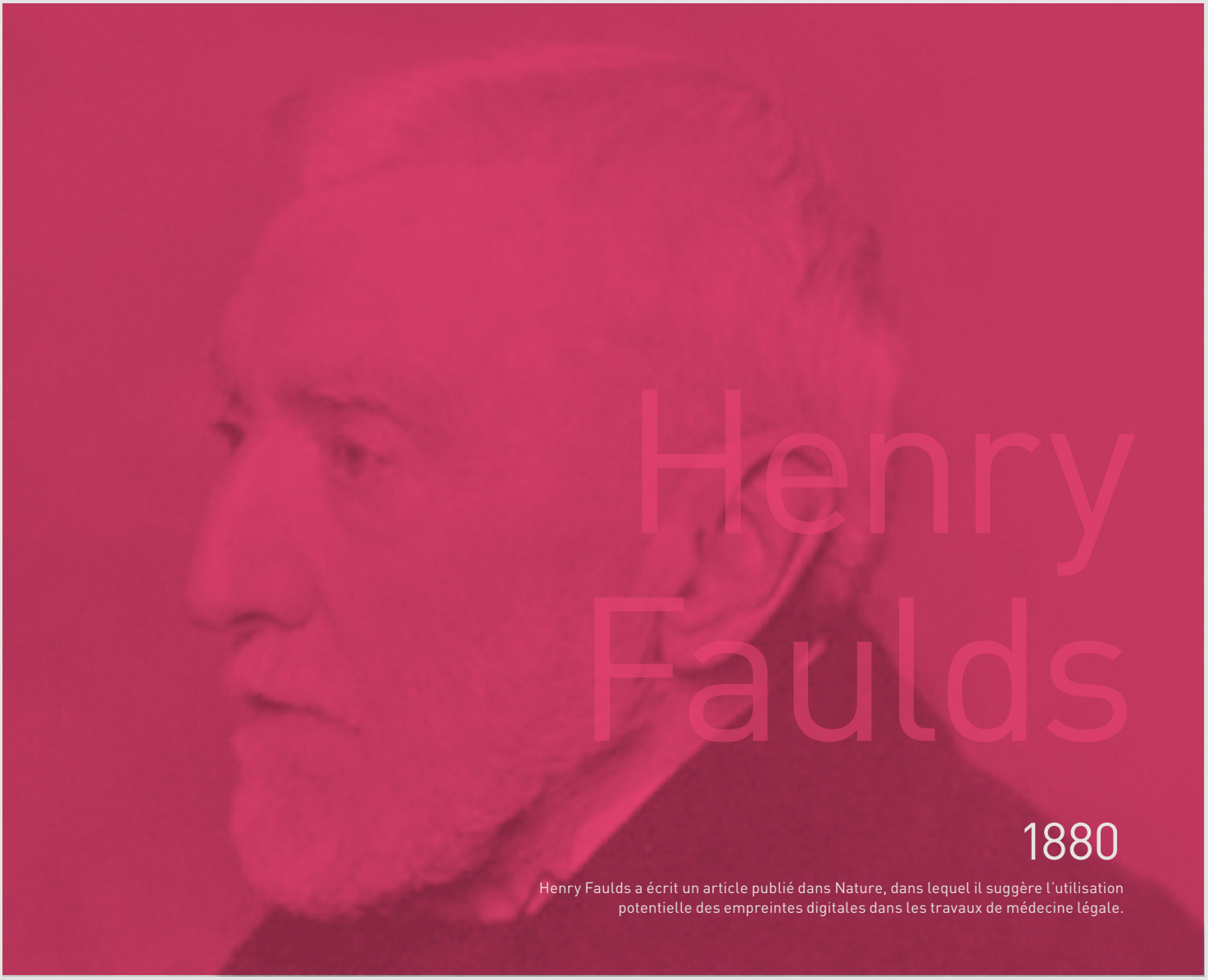
L'utilisation de la biométrie comme méthode d'authentification n'est pas nouvelle, car les caractéristiques physiques ont toujours été utilisées pour identifier les personnes. Il existe des preuves de l'utilisation des empreintes digitales comme authentification d'une personne dans des transactions commerciales babyloniennes et chinoises remontant respectivement à 500 et 300 ans avant Jésus-Christ. À la fin des années 1600, un certain nombre d'observations ont été faites sur les détails des empreintes digitales et, en 1788, l'anatomiste et médecin allemand J. C. A. Mayer a été le premier à déclarer le caractère unique de la crête papillaire.

Dans les années 1800, un anthropologue parisien, Alphonse Bertillon, a mis au point une méthode d'identification criminelle. Le "bertillonnage" exigeait des mesures nombreuses et précises de l'anatomie, de la forme du corps et des marques d'un être humain. À la fin du XIXe siècle, Sir Francis Galton a publié une étude détaillée dans laquelle il présentait un nouveau système de classification des empreintes digitales et les "minuties" qu'il a définies sont toujours utilisées. En 1896, la "méthode Henry" a été mise au point par Azizul Haque en Inde pour classer et stocker les empreintes digitales afin de pouvoir effectuer des recherches facilement et efficacement.

LA RECONNAISSANCE DES EMPREINTES DIGITALES



Les processus automatisés de reconnaissance biométrique ne sont devenus possibles qu'au cours des dernières décennies grâce aux progrès des circuits intégrés et du traitement informatique. Il existe aujourd'hui **une grande variété de technologies biométriques, la reconnaissance des empreintes digitales** étant la plus répandue.



Henry Faulds

1880

Henry Faulds a écrit un article publié dans Nature, dans lequel il suggère l'utilisation potentielle des empreintes digitales dans les travaux de médecine légale.

QU'EST-CE QUI EST NÉCESSAIRE POUR S'AUTHENTIFIER?

Les facteurs d'authentification nous donnent les moyens de vérifier l'identité ou de confirmer l'autorisation d'effectuer une tâche. Ils peuvent être regroupés en trois catégories de base : quelque chose que l'utilisateur sait, quelque chose que l'utilisateur a, ou quelque chose que l'utilisateur est.

INHÉRENCE

Quelque chose que l'utilisateur est ou fait, par exemple une empreinte digitale, une signature, une voix. L'authentification biométrique exploite divers facteurs d'hérédité pour valider l'identité d'un utilisateur.

PROPRIÉTÉ

Quelque chose que l'utilisateur possède, par exemple une carte d'identité, un jeton de sécurité, un téléphone portable, une clé, etc.

SAVOIR

Quelque chose que l'utilisateur connaît et dont il espère se souvenir, comme un mot de passe, un code PIN, la réponse à une question de sécurité, etc.

L'authentification comprend souvent au moins deux, voire trois des catégories ci-dessus. On parle alors d'authentification à deux ou plusieurs facteurs. Il est bien sûr également possible d'utiliser plusieurs facteurs de la même catégorie, comme un code PIN et une question de sécurité, mais cela ne donnera pas le même niveau de sécurité étendu qu'une "véritable" authentification multifactorielle.

LA BIOMÉTRIE EST-ELLE LA MEILLEURE SOLUTION ?

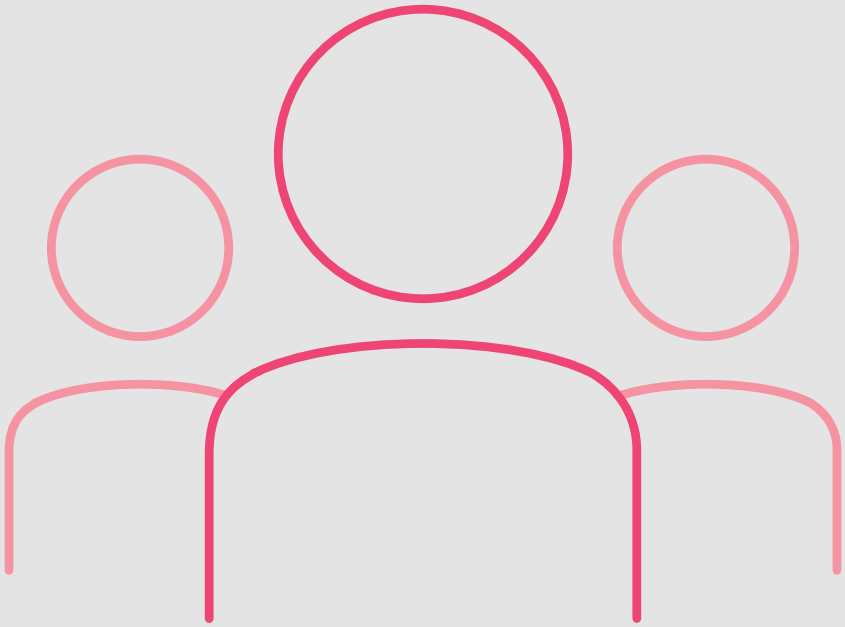
Lorsque l'on compare l'authentification biométrique à d'autres facteurs d'authentification, plusieurs aspects entrent en jeu. L'authentification basée sur des facteurs de connaissance (par exemple un mot de passe) est techniquement facile à mettre en œuvre mais aussi relativement facile à casser avec des algorithmes informatisés ou avec des logiciels espions dans l'appareil de l'utilisateur. De plus, les utilisateurs ont tendance à choisir des mots de passe simples et courants, voire à les partager avec d'autres. Cela rend impossible une authentification fiable. L'authentification basée sur des facteurs de propriété est généralement plus sûre, mais elle repose sur un jeton physique tel qu'une clé, une carte ou un téléphone, qui sont faciles à voler, à perdre ou même à laisser chez soi.

La fabrication de ces appareils coûte également de l'argent.

BIOMÉTRIE	AUTRES AUTHENTIFICATIONS
+ POSITIF	**+ POSITIF**
→ Unique à chaque personne → Toujours avec vous → Ne change pas à travers le temps	**SAVOIR** → Facile de mise en œuvre **PROPIÉTÉ** → Généralement plus simple
– NEGATIF	**– NEGATIF**
→ Acceptabilité sociale des méthodes biométriques → Le coût, la taille et les besoins en énergie du capteur et de la logique de traitement	**SAVOIR** → Des algorithmes faciles à casser → Les utilisateurs ont tendance à choisir des mots de passe simples et courants, voire à utiliser le même pour le bureau et pour la vie privée, et à les partager avec d'autres. Cela rend impossible une authentification fiable **PROPRIÉTÉ** → Repose sur un jeton physique qui est facile à perdre ou à voler

Ces avantages clés font de l'authentification biométrique l'outil privilégié de nombreuses applications. Il existe cependant quelques inconvénients, notamment la commodité et l'acceptabilité sociale de certaines méthodes biométriques. En outre, selon le type de biométrie utilisé, le coût, la taille et les besoins en énergie du capteur et de la logique de traitement peuvent constituer un inconvénient potentiel.

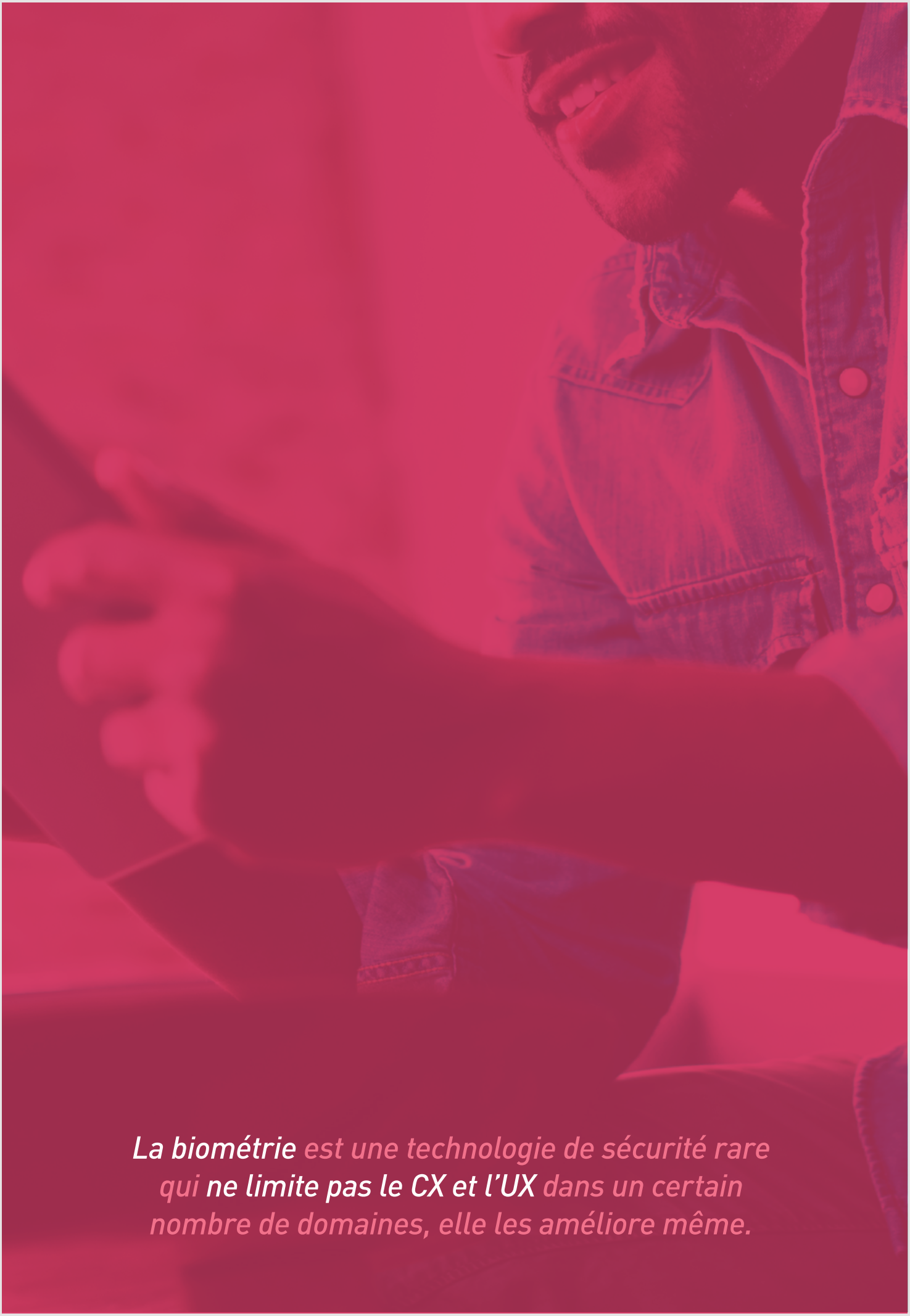
Dans le cas d'une authentification biométrique correctement mise en œuvre, les informations nécessaires sont **uniques pour chaque personne,** toujours présentes et ne changent normalement pas au fil du temps.



ALLIER SÉCURITÉ ET COMMODITÉ

La sécurité est évidemment l'un des facteurs les plus fondamentaux à aborder lors de la comparaison des systèmes d'authentification biométrique. Comme toujours, il faut trouver un compromis entre une sécurité élevée et le confort de l'utilisateur. L'évaluation de la sécurité d'un système ne se limite pas à la capacité de lecture et de comparaison de l'identifiant biométrique. Il faut également tenir compte de la possibilité d'un accès illégal au moteur de traitement (piratage) et de la possibilité d'être trompé par une personne simulant l'identifiant biométrique (usurpation).

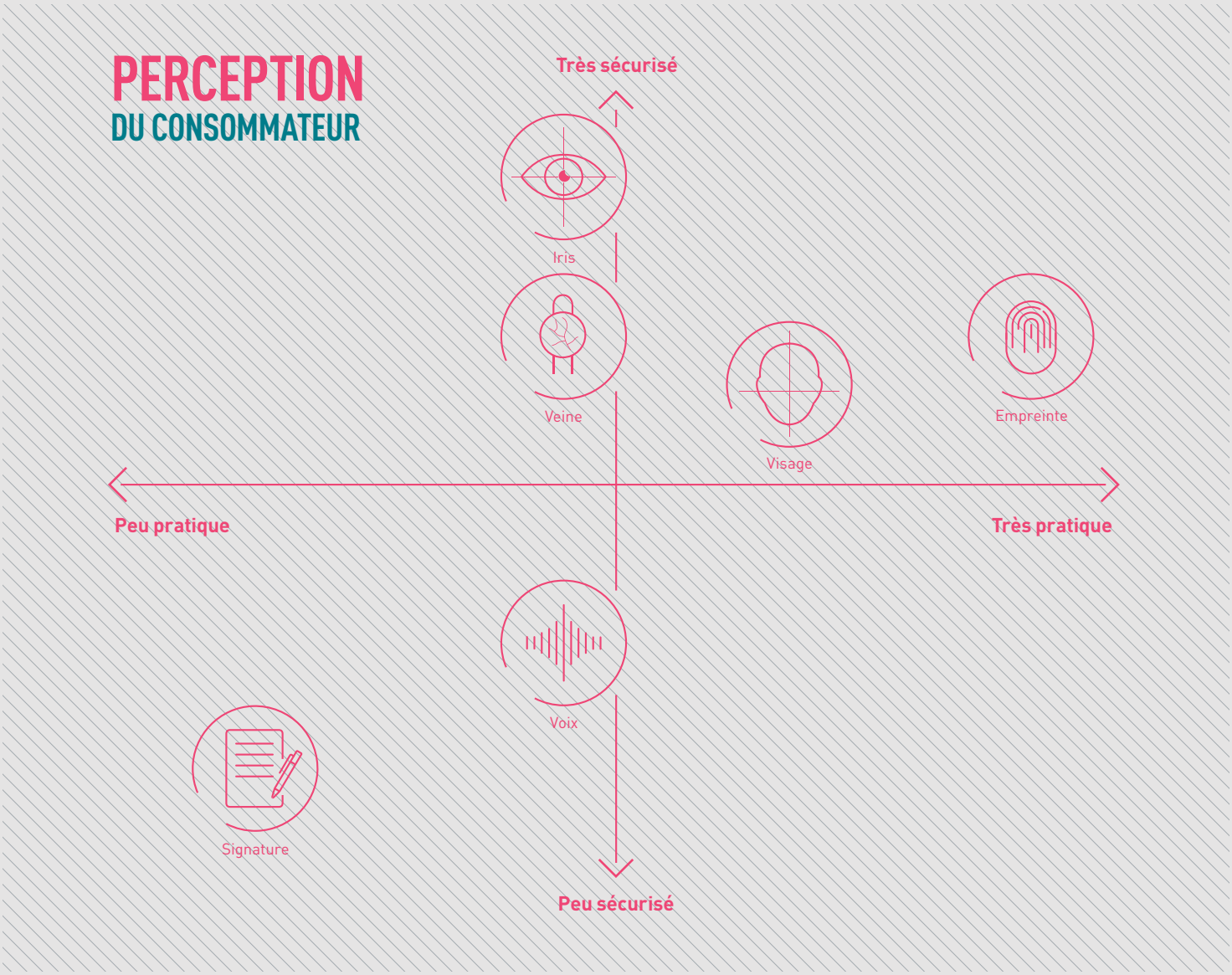
À titre d'exemple de mesure anti-piratage utilisée dans les appareils grand public modernes, une représentation mathématique de l'empreinte digitale est stockée comme modèle, au lieu de l'image elle-même. Le stockage de la représentation réduit les risques de piratage, car elle ne peut pas être utilisée pour recréer l'image originale de l'empreinte digitale. En outre, le modèle n'est pas stocké n'importe où sur l'appareil. Dans les appareils mobiles, le modèle est stocké et les algorithmes impliqués dans le processus d'authentification sont exécutés dans un environnement d'exécution de confiance (TEE). Cela renforce encore la sécurité, car les données biométriques, ainsi que les processus, restent à l'abri des pirates et des virus potentiels.



La biométrie est une technologie de sécurité rare qui ne limite pas le CX et l'UX dans un certain nombre de domaines, elle les améliore même.

De même, les cartes de paiement sont équipées d'un Secure Element, c'est-à-dire d'une puce qui offre un environnement dynamique pour stocker, traiter et communiquer des informations biométriques en toute sécurité. Si vous tentez d'altérer la puce de quelque manière que ce soit, elle peut s'autodétruire, mais ne vous permettra pas d'obtenir un accès non autorisé.

L'usurpation d'identité consiste à falsifier des visages, des voix, des empreintes digitales, dans le but de s'authentifier frauduleusement. De nombreuses technologies avancées ont été développées pour minimiser le risque d'usurpation. Dans la reconnaissance des empreintes digitales, les risques d'usurpation peuvent être réduits en augmentant la qualité de l'image et en utilisant des algorithmes de correspondance sophistiqués. Une sécurité supplémentaire peut être obtenue grâce à divers mécanismes de lutte contre l'usurpation d'identité et à l'utilisation de plus d'un identifiant biométrique pour authentifier l'utilisateur.



Source: Fingerprints™ market reseach 2017 en collaboration with Kantar TNS, 4,000 consommateurs en ligne UK, USA, Chine, Inde.

Aucun système ne peut être rendu absolument sûr - avec un temps (et un argent) illimité, vous pouvez pirater et falsifier n'importe quoi. Les techniques biométriques avancées rendent toutefois ces attaques malveillantes extrêmement coûteuses et fastidieuses.

TFR VS TFA

Le tracé du TFR en fonction du TFA pour différents types de systèmes d'authentification biométrique donne un aperçu des compromis entre sécurité et commodité. Le capteur idéal a un TFA et un TFR minime, mais en réalité, les systèmes d'authentification biométrique se situent quelque part sur une courbe où l'on a une grande commodité (TFR faible) mais une sécurité moindre (TFA élevé) et vice versa.

La commodité est également liée à d'autres attributs du capteur, tels que l'intuitivité de son utilisation, la rapidité de son réveil/la manière dont l'utilisateur le réveille, ainsi que la manière dont le capteur est intégré au produit final, bien que cela soit davantage une conséquence de la taille et de la flexibilité de la conception du capteur.

Mais quels sont les types d'authentification biométrique et **pourquoi l'empreinte digitale s'est-elle imposée ?**

CHAPITRE 02

02

Qu’est-ce qui fait de l’empreinte digitale la reine ?

QU'EST-CE QUI FAIT DE L'EMPREINTE DIGITALE LA REINE ?

Les êtres humains possèdent de nombreux identifiants biométriques, ou modalités, qui peuvent être capturés et analysés par les systèmes biométriques. Les identificateurs comportementaux sont des traits mesurables acquis au fil du temps et qui peuvent être analysés pour confirmer l'identité en utilisant des techniques de reconnaissance des formes. Les modalités physiologiques sont quelque chose que vous êtes, plutôt que quelque chose que vous faites ou savez

EXEMPLES D' **IDENTIFICATIONS PSYCOLOGIQUES**	EXEMPLES D' **IDENTIFICATIONS COMPORTEMENTALES**
Empreintes digitales : doigt, main, pied	Voix
Iris et rétine	Signature
Visage, oreilles	Gestuelle
Schémas veineux et vasculaires	Démarche

EMPRUNTE DIGITALE

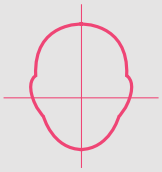
Analyse des crêtes et des motifs uniques de la peau du bout des doigts.

Hautement unique, facile à collecter, très mesurable et généralement permanente tout au long de la vie d'une personne, il existe également un certain nombre de normes déjà en place. Cela a fait de l'empreinte digitale la modalité de facto à ce jour, bien que certains la trouvent intrusive et que des difficultés subsistent lorsque les doigts sont sales ou particulièrement secs/humides.

YEUX

Examen de l'iris, de la rétine ou des veines sclérales de l'œil

Comme les empreintes digitales, les caractéristiques des yeux sont uniques et permanentes. Par le passé, cette technologie était souvent utilisée par les pouvoirs publics, notamment pour le contrôle des frontières, mais grâce à de nouvelles avancées et à des processus d'inscription plus simples, elle est désormais utilisée dans des appareils grand public tels que les smartphones. Elle fonctionne désormais aussi dans des conditions plus sombres et avec des lunettes.



VISAGE

Examen des nombreuses caractéristiques du visage

Relativement peu coûteuse à mettre en œuvre à l'aide d'un appareil photo ou de la technologie actuelle des smartphones, la reconnaissance faciale peut se faire sur des distances beaucoup plus grandes que certaines autres modalités. Elle peut toutefois être assez facile à falsifier, nécessite un bon éclairage et sa faible stabilité dans le temps, car le visage change, peut entraîner un taux d'échec élevé. La dernière technologie 3D a amélioré la sécurité, mais elle a un coût élevé.

VOIX

Analyse de l'empreinte vocale d'une personne

Bien qu'elle soit facile à mettre en œuvre et peu coûteuse, elle présente des inconvénients majeurs. Les empreintes vocales évoluent avec le temps et nécessitent des mises à jour régulières. Elles peuvent également changer en raison de facteurs tels que l'environnement et la maladie. Les empreintes vocales peuvent être facilement enregistrées et falsifiées. Il convient également de tenir compte de l'interface utilisateur, car demander à l'utilisateur de parler peut prendre du temps et s'avérer peu pratique. En revanche, la voix est parfaite en tant qu'interface utilisateur, car elle constitue un moyen pratique et naturel d'interagir avec divers appareils.

RECONNAISSANCE DES VEINES

Examen du réseau veineux des doigts ou des mains.

La veine est une méthode hautement sécurisée ; le schéma vasculaire se trouve sous la peau. Les scanners, cependant, peuvent être assez grands, coûteux et nécessitent beaucoup d'énergie. Le processus de comparaison peut également être assez lent, car les schémas veineux sont très complexes, ce qui rend les exigences de traitement très élevées.

COMPORTEMENT

Examen du réseau veineux des doigts ou des mains.

La mesure précise des paramètres de la marche nécessite un équipement sophistiqué, comprenant plusieurs techniques, ce qui la rend coûteuse et compliquée à mettre en œuvre. Les gestes peuvent également être interprétés, mais cette technologie n'en est qu'à ses débuts et les problèmes de sécurité et d'usurpation d'identité doivent encore être résolus. Elle peut être utilisée en arrière-plan comme deuxième ou troisième facteur pour renforcer la sécurité dans des cas d'utilisation tels que les transactions en ligne ou, à l'avenir, les magasins shop & go.

COMPARER LES MODALITÉS BIOMÉTRIQUES

		EMPREINTE	IRIS	VISAGE (2D)	VISAGE (3D)	VEINES	VOIX
SECURITE	Unique	Moyen	Haut	Bas	Moyen	Haut	Bas
	Dur à copier/frauder	Moyen	Haut	Bas	Moyen	Haut	Bas
COMMODITE	Vitesse	Haut	Moyen	Moyen	Moyen	Moyen	Bas
	Précision	Moyen	Haut	Bas	Moyen	Haut	Moyen
ADAPTABILITÉ	Rentabilité	Moyen	Moyen	Haut	Bas	Moyen	Haut
	Facile à intégrer	Haut	Haut	Haut	Bas	Bas	Haut

Haut Moyen Bas

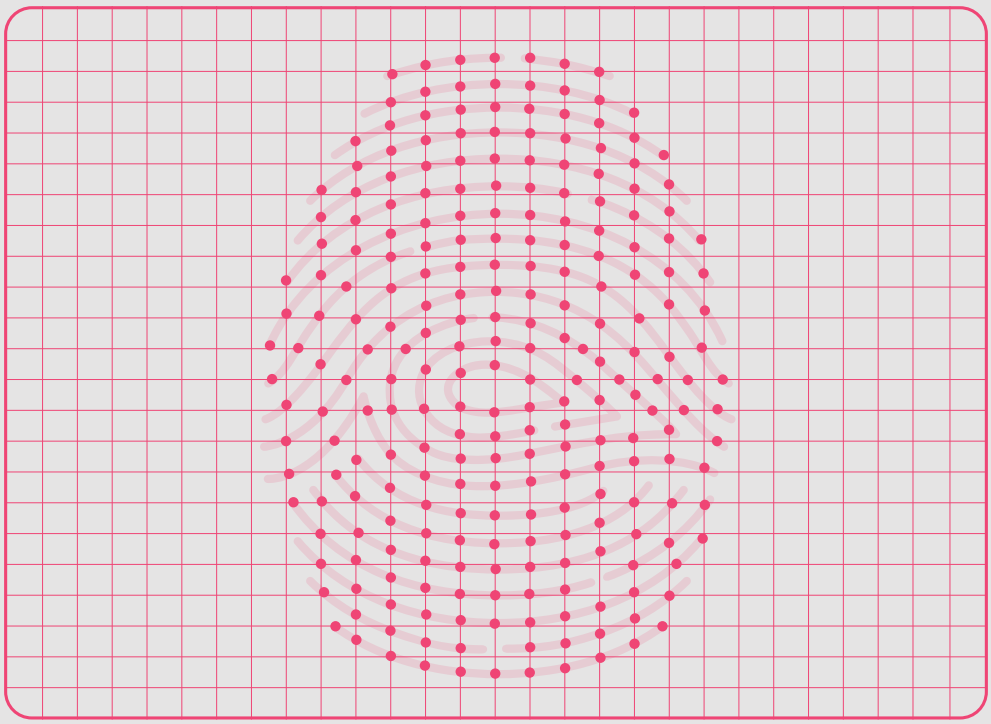
On peut donc dire que les entreprises qui cherchent à mettre en œuvre l'authentification biométrique ont plusieurs options, en fonction de leurs besoins.

UN REGARD PLUS ATTENTIF SUR L'EMPREINTE DIGITALE

Malheureusement, il ne s'agit pas simplement de choisir « une empreinte digitale », car il existe plusieurs types de capteurs d'empreintes digitales qui se prêtent chacun à différents cas d'utilisation et scénarios.

QU'EST-CE QU'UN CAPTEUR D'EMPREINTES DIGITALES ?

Un capteur digital est un dispositif électronique utilisé pour enregistrer une image numérique du motif de l'empreinte digitale. Il est souvent intégré à un autre appareil, comme un smartphone, un ordinateur portable, une carte de paiement ou une serrure de porte. Le capteur capture les caractéristiques pertinentes de l'empreinte digitale pour un traitement ultérieur dans l'appareil.



CAPACITIF - génère l'image de l'empreinte digitale en faisant passer un petit courant électrique sur la surface du doigt.

L'excellente qualité d'image permet de produire à faible coût de petits capteurs à très faible consommation d'énergie. Ils renforcent également les mesures anti-usurpation 3D, permettent une capture d'image rapide, sont durables et faciles à intégrer. Avec la possibilité de produire des capteurs de très petite taille, il est essentiel que l'inscription et la vérification soient effectuées avec soin et avec un logiciel de haute qualité. Cette technologie est en passe de devenir le capteur d'empreintes digitales le plus courant et le plus populaire dans les appareils grand public tels que les smartphones.

OPTIQUE - Une caméra est utilisée pour capturer l'image de l'empreinte digitale.

En tant que premier capteur d'empreintes digitales, ils sont désormais peu coûteux à produire et peuvent également être intégrés à l'écran, ce qui ouvre de nouveaux cas d'utilisation, comme les capteurs intégrés à l'écran des smartphones. Mais ils sont également sujets à l'usurpation, ne fonctionnent pas bien à la lumière du soleil, sont sensibles à la contamination par leur environnement et s'usent souvent avec l'âge.

THERMIQUE - Crée des images d'empreintes digitales en utilisant des mesures de température.

Leur adoption est limitée car ils ont souvent des besoins énergétiques élevés, ne sont pas capables de capturer des détails fins, peuvent être assez grands, ne peuvent pas créer d'images en 3D et sont sensibles à l'usure.

ULTRASONIQUE - Crée des images visuelles de l'empreinte digitale en faisant rebondir des ondes sonores à haute fréquence sur la couche épidermique de la peau.

Ils fournissent plus d'informations biométriques que la plupart des autres capteurs d'empreintes digitales et sont capables de lire les doigts humides et endommagés, mais pas les doigts secs. Ils peuvent être lents, coûteux, gourmands en énergie, encombrants et nécessiter une grande puissance de traitement.

PRESSION - Crée une image lorsque les crêtes et les vallées d'un doigt appliquent différents niveaux de pression sur la surface.

Les capteurs sensibles à la pression peuvent être de petite taille et constituent l'une des rares catégories de capteurs, à côté des capteurs capacitifs, qui peuvent être intégrés dans des appareils plus petits tels que les téléphones mobiles et les tablettes. Cependant, les capteurs existants sont sensibles à la température et sont moins adaptés à une utilisation dans des conditions environnementales difficiles ou changeant rapidement.

La biométrie est utilisée pour déverrouiller les appareils mobiles, accéder aux applications et vérifier les paiements.
La confiance et l'utilisation du mobile ouvrent la voie à l'intégration dans de nouveaux appareils et applications.

POUR PARVENIR À UNE ADOPTION MASSIVE PAR LE MARCHÉ, LES CARACTÉRISTIQUES SUIVANTES SONT ESSENTIELLES:

QUALITÉ & RÉSOLUTION DE L'IMAGE

Les images de haute qualité permettent de produire des capteurs plus petits. Cela est possible en grande partie grâce aux capteurs à ultrasons et aux capteurs capacitifs actifs.

VITESSE

La vitesse de fonctionnement a une corrélation directe avec la commodité et l'expérience de l'utilisateur. Les capteurs capacitifs, thermiques et de pression peuvent tous fonctionner très rapidement.

CONSOMMATION D'ÉNERGIE

Les exigences de faible consommation sont fondamentales pour les appareils portables tels que les smartphones et les cartes à puce. Les capteurs capacitifs ont actuellement la plus faible consommation d'énergie.

TAILLE

Les petits capteurs s'intègrent plus facilement dans les appareils et coûtent moins cher. Les capteurs capacitifs actifs permettent d'obtenir le meilleur compromis entre taille et qualité d'image.

COUT

Facteur clé de l'adoption généralisée dans les téléphones moins chers, les cartes à puce et autres appareils à grand volume.

PACKAGING & DESIGN

Les capteurs doivent pouvoir compléter la conception de l'appareil et les capteurs capacitifs actifs offrent le plus de flexibilité. Comme ils ont une empreinte plus petite, ils laissent plus de place au design de l'id et peuvent être intégrés dans de très petits dispositifs comme une carte.

SÉCURITÉ & COMMODITÉ

Trouver le bon équilibre est essentiel pour garantir l'utilisation d'une authentification forte. Les capteurs capacitifs actifs peuvent offrir de faibles taux de faux rejets et d'approbation.

Le coût, l'efficacité énergétique, la taille, la commodité et d'autres exigences font qu'il n'y a pas de "gagnant" pour chaque appareil et chaque scénario. Cependant, si l'on considère le marché, la technologie capacitive présente une série de caractéristiques attrayantes qui en font un premier choix dans la plupart des applications.

COMPARAISON DES TECHNOLOGIES D'EMPREINTES DIGITALES

	CAPACITIF ACTIF	ULTRASONIQUE	OPTIQUE	THERMIQUE ACTIF
Efficacité des coûts	Moyen	Faible	Faible	Faible
Flexibilité du design	Haut	Faible	Faible	Faible
Maturité technologique	Haut	Moyen	Haut	Moyen
Securité	Moyen	Moyen	Faible	Moyen
Commodité	Haut	Faible	Faible	Faible
Efficacité énergétique	Haut	Moyen	Moyen	Faible
Adoption d'appareils mobiles	Haut	Faible	Moyen	Faible

Haut Moyen Faible

CHAPITRE 03

03

Le succès de l'empreinte digitale dans la téléphonie mobile

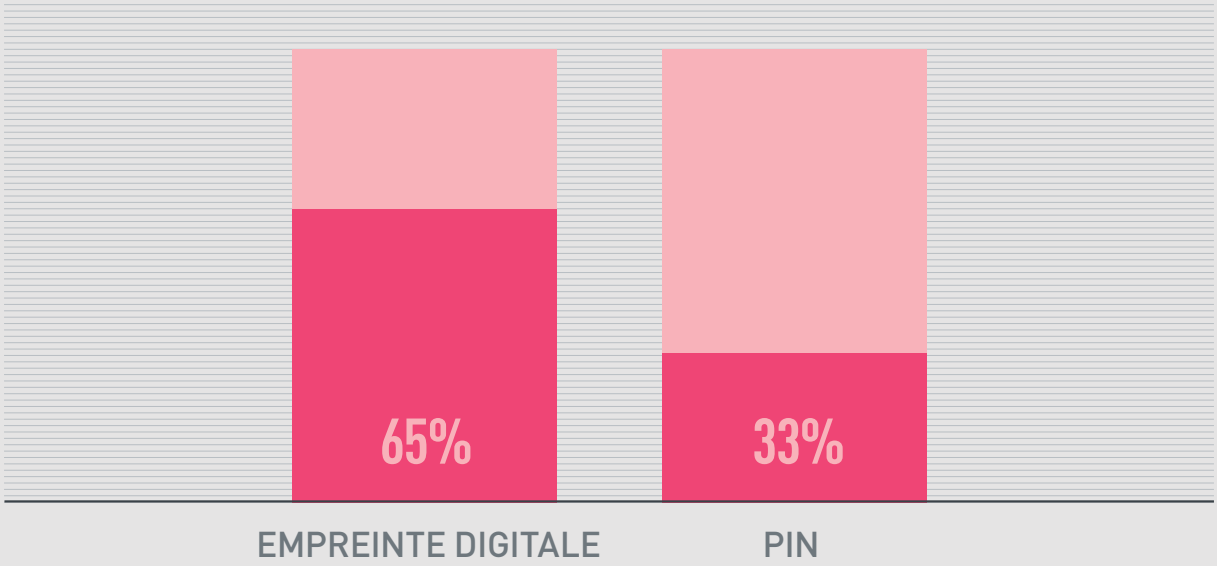
LE SUCCES DE L'EMPREINTE DIGITALE DANS LA TELEPHONIE MOBILE

Les portables sont au cœur de notre vie quotidienne, mais ils ne servent plus seulement à téléphoner et à envoyer des SMS. Nous les utilisons désormais pour les voyages, les paiements, les courriels et les opérations bancaires, et chaque nouveau cas d'utilisation s'accompagne d'informations encore plus sensibles.

Lorsque vous combinez l'erreur humaine et la paresse avec les exigences actuelles en matière de mots de passe complexes (Attention : le mot de passe doit comporter au moins 12 caractères et contenir une majuscule, un chiffre, un caractère spécial et ne peut pas contenir un mot, un nom ou un lieu), vous obtenez la recette du désastre.

Tout cela a permis à la biométrie de s'imposer comme l'une des meilleures solutions d'authentification pour faire rimer sécurité mobile avec commodité.

L'EMPREINTE DIGITALE EST DÉSORMAIS PLUS UTILISÉE QUE LE CODE PIN LORSQU'IL EST DISPONIBLE SUR LE SMARTPHONE



>80%

80% des smartphones expédiés sont équipés de la biométrie

23%

23% utilise la biométrie pour authentifier les paiements mobiles

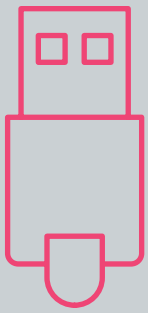
Les capteurs d'empreintes digitales devraient également rester l'option d'authentification numéro un, malgré les autres solutions - comme les scanners d'iris et la reconnaissance faciale - qui ont fait la une des journaux.

Source : Fingerprints en collaboration avec Kantar Décembre 2019 (1,200 consommateurs en ligne en Chine, France, UK)

NOUVEAUX CAS D'UTILISATION DES PAIEMENTS

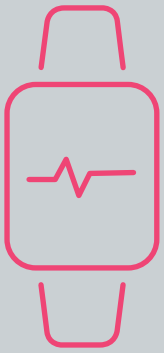
Nous avons établi que la reconnaissance des empreintes digitales est la modalité prédominante - et que les capteurs capacitifs offrent la plus grande flexibilité en termes de taille, de sécurité, de commodité, de consommation d'énergie et de coût - il n'est donc pas surprenant que les nouveaux appareils intègrent des capteurs capacitifs.

L'authentification forte devenant de plus en plus importante sur les appareils, en magasin et en ligne, de plus en plus d'appareils peuvent bénéficier de la prise en charge d'un capteur biométrique.



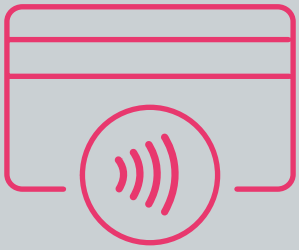
PRISE USB

Apporter une authentification physique forte aux achats et services en ligne



OBJETS CONNECTES

Protégez le déverrouillage des appareils et le paiement des articles vestimentaires d'une simple pression



CARTE DE PAIEMENT

Faire confiance aux cartes de paiement sans contact et supprimer le plafond de paiement

Ces cas d'utilisation et d'autres encore **intègrent déjà des capteurs d'empreintes digitales.** Les cartes de paiement biométriques peuvent apporter d'énormes avantages aux consommateurs, aux banques et aux détaillants.

CHAPITRE 04

04

Adaptation de la technologie mobile aux cartes de paiement

ADAPTATION DE LA TECHNOLOGIE MOBILE AUX CARTES DE PAIEMENT

L'empreinte digitale est, bien entendu, le seul moyen d'authentification biométrique viable pour les cartes de paiement en plastique en raison de leur taille, de leur puissance et d'autres limitations. Mais la route a été longue pour en arriver là. Les systèmes biométriques mobiles étaient trop gros, trop épais et trop gourmands en énergie pour être intégrés dans les cartes à puce et une quantité énorme de R&D a été consacrée à la réduction de la taille du matériel et du logiciel.

En raison des exigences uniques des cartes à puce, les points suivants ont dû être pris en compte et traités :

01. PROCESSUS DE FABRICATION

Pour faciliter l'adoption, il était essentiel que l'intégration d'un capteur d'empreintes digitales n'ait pas d'impact significatif sur les processus de fabrication des cartes standard. Nous avons donc conçu un module de capteur qui peut être facilement pris en charge par les machines actuelles.

02. SYSTÈME SUR CARTE

Pour une sécurité et une confidentialité maximales, il était important que le stockage, le traitement et la correspondance des modèles soient effectués sur la carte elle-même, une approche déjà largement acceptée dans le monde de l'identification.

03. TAILLE DES CAPTEURS

Il a fallu beaucoup de travail pour obtenir un capteur suffisamment fin et petit pour fonctionner parfaitement dans une carte en plastique. Mais nous nous sommes également efforcés d'améliorer la qualité du capteur lui-même afin de réduire l'empreinte sur la face de la carte et de maximiser l'espace pour l'image de marque et le design.

04. FLEXIBILITÉ DU MATÉRIEL

Les smartphones ne se plient pas (encore), mais les cartes, si. En fait, elles doivent passer de vigoureux tests de qualité et de flexibilité. C'est là qu'intervient notre conception révolutionnaire T-Shape™.

05. QUALITÉ DE L'IMAGE

Pour obtenir la meilleure image possible, le matériel et le logiciel doivent fonctionner en parfaite harmonie. Il s'agit de trouver le point idéal en obtenant la meilleure image possible avec le plus petit capteur, le plus rapidement et en utilisant la plus faible puissance. Il s'agit d'obtenir la meilleure interface utilisateur avec le moins de faux rejets possible.

06. BAISSE CONSOMMATION D'ÉNERGIE

Tout doit fonctionner aussi précisément et rapidement que possible en utilisant uniquement l'énergie empruntée au terminal de paiement, de sorte qu'il n'y a pas besoin de batterie dans les cartes. Nous avons donc tout optimisé pour fonctionner avec la plus faible puissance disponible sur certains terminaux. S'il y a plus d'énergie disponible, nos algorithmes fonctionnent encore plus vite !

07. QUALITÉ DU LOGICIEL

Les gens se concentrent souvent sur le matériel, mais c'est dans le logiciel que la vraie magie opère. Prévention des fraudes, amélioration de l'image, mises à jour intelligentes des modèles - la qualité du logiciel fait la différence entre tap&go et tap&slow.

08. LATENCE BASSE

Les acheteurs n'ont pas le temps, donc avoir un processeur qui doit démarrer n'était pas une option que nous étions prêts à envisager. Notre capteur est toujours en veille et prêt à fonctionner.

09. CONNECTIVITÉ SÉCURISÉ

L'élément sécurisé et le capteur d'empreintes digitales sont des unités distinctes, mais la sécurité est fondamentale. Nous avons donc travaillé dur avec nos partenaires pour nous assurer que la connectivité sécurisée répond aux mêmes niveaux que dans le monde des smartphones.

10. ENROLLEMENT

Il ne peut y avoir qu'une seule façon de s'inscrire, les banques ont des préférences différentes et les consommateurs aussi. Il était donc essentiel d'envisager des options d'inscription flexibles. Le processus a été soigneusement étudié pour le rendre aussi facile que possible pour les titulaires de cartes.

Notre vaste expérience dans le domaine de la téléphonie mobile nous a permis d'examiner chaque aspect du système biométrique et de l'optimiser pour une utilisation sur les cartes de paiement. En fait, certains aspects du matériel et du logiciel sont aujourd'hui si avancés que nous ne les utilisons pas encore à leur plein potentiel. Cela nous sera précieux à l'avenir.

CHAPITRE 05

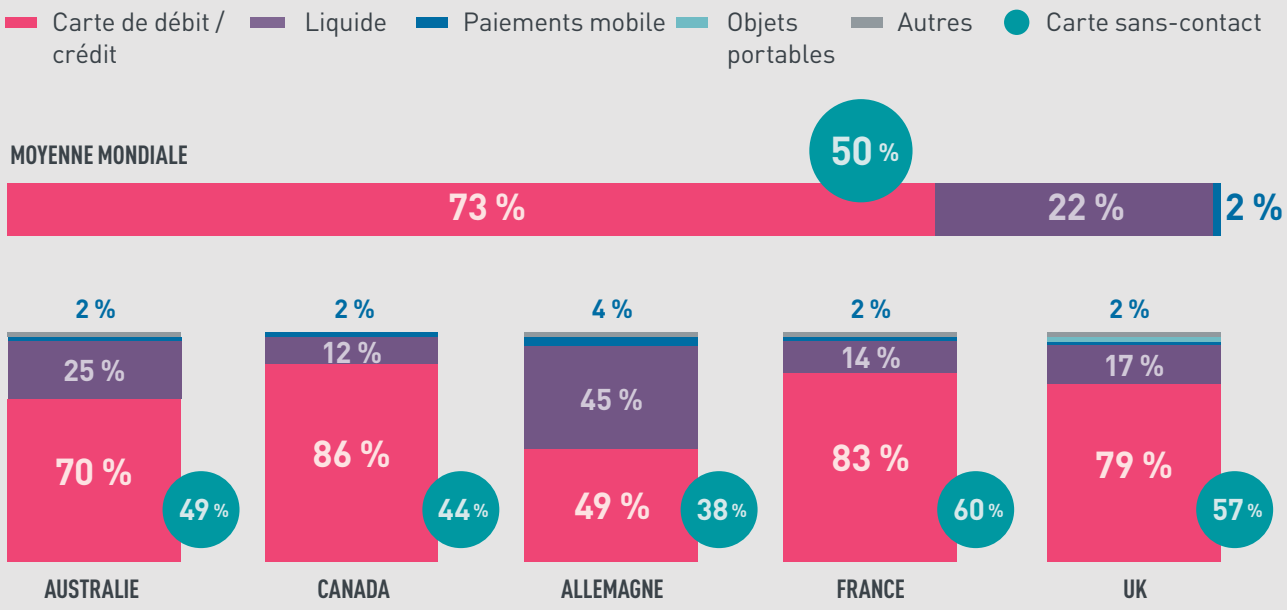
05

Cartes de paiement - le prochain cas d’utilisation

CARTES DE PAIEMENT - LE PROCHAIN CAS D'UTILISATION

La carte reste le moyen de paiement le plus populaire dans le monde, et son utilisation augmente d'année en année, malgré la possibilité de payer par téléphone intelligent.

LA CARTE SANS CONTACT EST LE MOYEN PRÉFÉRÉ DES CONSOMMATEURS POUR PAYER EN MAGASIN



Source : Fingerprints™ en collaboration avec Kantar Sep 2020 (2,000 consommateurs en ligne en Australie, Canada, Allemagne, France, UK)

Mais l'adoption du sans contact reste un défi, 51 % des personnes interrogées déclarant que le sans contact n'est pas sûr et 49 % étant très préoccupées par la fraude.

Heureusement, la technologie est désormais disponible pour intégrer la biométrie aux cartes de paiement. Les consommateurs bénéficient ainsi de la rapidité et de la commodité des paiements sans contact, avec en plus la confiance et la sécurité de l'authentification biométrique.

Mais quels sont les bénéfices ?

SUPPRIMER LE PLAFONNEMENT DES PAIEMENTS

Le plafond de paiement de 50 £ (Royaume-Uni), 50 € (France) et 200 $ (Canada, Australie) sur les cartes sans contact standard peut constituer un autre obstacle à la vente. Grâce au niveau de sécurité plus élevé des cartes de paiement biométriques, ce plafond pourrait être supprimé.

Les consommateurs apprécieront la commodité accrue du sans contact pour chaque achat, associée à l'assurance de l'authentification biométrique. Ce qui devrait augmenter à la fois les dépenses et le débit des commerçants et d'autres entreprises telles que les restaurants. Le fait que les consommateurs dépensent davantage avec leurs cartes de débit/crédit est également une bonne nouvelle pour les revenus des banques.

NOUVELLES CARTES, TPE IDENTIQUES

Dans les régions où les dernières technologies sont considérées comme un symbole de statut social, les cartes de paiement biométriques présentent un attrait naturel.

Dans d'autres régions, la technologie avancée permettra aux banques d'accroître leur statut et la confiance des consommateurs en montrant qu'elles sont à l'avant-garde avec une nouvelle technologie. Une expérience financière plus positive profitera au consommateur, tout en aidant les banques à attirer de nouveaux clients et à fidéliser les anciens.

Il est important de noter que cette avancée technologique n'a pas de coût pour les détaillants, puisqu'il n'est pas nécessaire de mettre à niveau leurs terminaux de paiement sans contact existants.

UNE MEILLEURE INCLUSION FINANCIÈRE

Les cartes à puce et à code PIN, ou celles qui nécessitent une signature, peuvent également poser problème à diverses personnes, notamment celles qui:

- Sont analphabète
- Utilisent des séries de chiffres différents
- Ont du mal à retenir leur code PIN

Les cartes de paiement biométriques permettent de surmonter ce problème car le titulaire de la carte n'a besoin que de son empreinte digitale pour prouver son identité.

Les banques ont la possibilité d'accroître l'inclusion financière en fournissant ces cartes aux personnes qui ne peuvent pas utiliser d'autres types d'authentification. Les services financiers peuvent être accessibles à une nouvelle base de consommateurs pour la toute première fois, ce qui signifie que les petites entreprises et les détaillants dans des zones auparavant peu accessibles verront les dépenses sur carte augmenter à un rythme sans précèdent.

DONNÉES AUTONOMES ET SÉCURISÉES

Sont stockés dans l'élément sécurisé de la carte :

- Modèle d'empreinte digitale du titulaire de la carte
- Données personnelles et de compte
- Des moteurs de comparaison qui vérifient l'authenticité de l'empreinte digitale présentée lors du paiement.

Les consommateurs gardent la main sur leurs données biométriques plutôt que de les confier à un tiers. Et s'ils perdent la carte, leurs données restent cryptées dans l'élément sécurisé où personne ne peut les utiliser.

PAS DE BATTERIES OU DE MISES À NIVEAU DES TERMINAUX

L'énergie du terminal de paiement alimente le capteur biométrique de la carte. La carte n'a pas besoin de piles ni de recharge et peut être utilisée avec les terminaux existants conçus pour les paiements sans contact ou à puce.

PEUVENT ÊTRE UTILISÉS MONDIALEMENT

Les systèmes de paiement garantissent que la carte fonctionne en toute sécurité et répond aux normes EMV et ISO actuelles. Ainsi, une carte de paiement biométrique émise par une banque dans un pays peut être utilisée pour effectuer des paiements en toute sécurité dans un autre pays.

UNE AUTHENTIFICATION SIMPLE ET PRODUCTIVE

Dans la carte, un capteur d'empreintes digitales ultra-mince, et de faible puissance. Vous pouvez le toucher sous n'importe quel angle, l'authentification est donc rapide et simple. La fabrication des cartes biométriques est également simple, car les capteurs sont intégrés dans les processus de fabrication existants.

CHAPITRE 06

06

Quelle est la prochaine étape ? Questions à poser à votre partenaire de carte

QUESTIONS A POSER A VOTRE PARTENAIRE DE CARTE

Avec autant d'options, les banques ont besoin d'un moyen de qualifier la meilleure technologie pour leurs besoins. Voici une liste de questions que les banques et les institutions financières doivent poser à leur fabricant de cartes afin de s'assurer qu'elles obtiennent la meilleure technologie pour leur profil de risque et leurs clients.

GÉNÉRAL

- Puis- je voir une demo en live du produit en action ?
- Quels essais et projets pilotes ont été menés à l'échelle mondiale et pouvez-vous nous faire part de vos commentaires ?

MATÉRIEL

- Offrez-vous un capteur à base de silicium? (Meilleure qualité – images 3D – vise plus de 500 points par pouce)
- Votre capteur est-il un capteur capacitif actif ? (Le meilleur compromis entre le coût, l'efficacité énergétique, la taille, la commodité, etc)
- Proposez-vous une solution de système sur carte ?
- De quelle taille est le capteur ? (Les capteurs plus petits laissent plus de place à votre marque)
- Le processeur doit-il démarrer ou est-il toujours prêt ? (Cela limite la latence, ce qui augmente la vitesse et la commodité)

LOGICIEL

- Quelle est la rapidité du processus de vérification ? (– d'une second)
- Quel est le FRR du produit ? Visez moins de 3 %.
- Quelles mesures de sécurité le produit offre-t-il ?
- Quelles sont les options d'inscription à la banque ou à domicile ?
- Combien de touches faut-il pour s'inscrire ? (Cela facilite la mise en route pour l'utilisateur)
- L'algorithme apprend-il à chaque contact ou l'inscription est-elle statique ?
  (Cela peut limiter les faux rejets)
- Le logiciel prend-il en charge la reconnaissance d'empreintes digitales à 360° ? (La bonne empreinte digitale doit être reconnue, quel que soit l'angle)

ET APRÉS ?

ET APRÉS ?

Il a fallu du temps et une expertise incroyable pour intégrer les capteurs d'empreintes digitales aux cartes à puce pour des utilisations telles que les paiements. Tout est désormais en place. En 2021 et au-delà, les cartes biométriques seront déployées par les banques et les institutions financières du monde entier, au bénéfice de leurs activités, des commerçants et des consommateurs.

Quel que soit le cas d'utilisation, les émetteurs doivent être en mesure d'évaluer les différentes technologies à leur disposition afin de pouvoir prendre des décisions éclairées qui leur apporteront un maximum d'avantages, à eux et à leurs clients. Quel type de capteur est le mieux adapté à nos besoins ? Quelle est l'efficacité du logiciel de prévention de la fraude ? Quelles sont les options d'enrôlement ? Quelles sont les fonctions supplémentaires disponibles qui maximisent la facilité d'utilisation au quotidien ? Tout cela a un impact sur la qualité du produit et l'expérience de l'utilisateur et, si ces éléments ne répondent pas aux exigences des consommateurs, l'adoption sera lente et l'argent gaspillé. La biométrie peut unifier l'authentification sécurisée du client sur toutes les formes de paiement, il s'agit simplement de choisir la bonne méthode.

À PROPOS DE NOUS ET DE NOS PARTENAIRES

DU SMARTPHONE À LA CARTE DE PAIEMENT

Plus de 30 grandes marques ont intégré nos capteurs dans plus de 500 modèles de smartphones. Au-delà, notre solution est également intégrée dans divers dispositifs IoT innovants utilisés pour l'authentification et les paiements sécurisés. Nous avons adapté cette technologie au succès retentissant avec notre module de capteur T-shape unique, conçu sur mesure pour les cartes de paiement. Fin et petit, il offre une haute qualité d'image avec des performances biométriques optimisées et éprouvées pour des surfaces plus petites telles qu'une carte de paiement. Et avec la meilleure consommation d'énergie de sa catégorie, il permet une authentification sans contact sans batterie. Nos capteurs peuvent être fabriqués de manière rentable et en grande quantité avec les processus de production de cartes standard. Ils peuvent également être laminés afin de ne pas compromettre le design de la carte.

COMMENT FAISONS NOUS DES CARTES DE PAIEMENT BIOMÉTRIQUES UNE RÉALITÉ ?

Le potentiel de la biométrie sur carte est énorme, mais nous ne pouvons pas le réaliser seuls. Nous collaborons avec un large éventail de représentants de l'écosystème des paiements (voir ci-dessous), qui ont tous un rôle essentiel à jouer.

LEADER DE LA BIOMÉTRIE

Fingerprints ouvre la voie. Grâce à notre expertise dans le domaine des capteurs de smartphones de grand volume, nous sommes à l'origine d'innovations qui permettront aux cartes de paiement biométriques d'atteindre le marché de masse.

APPORTENT DES SOLUTIONS

Comme STMicroelectronics, Infineon and NXP adapte et développe des composants, notamment des éléments sécurisés, des prélams et des inlays, pour répondre aux nouvelles exigences.

FABRIQUANTS DE CARTES

Comme Thales, Idemia, G+D développent et fabriquent des cartes de paiement biométriques et d'autres cartes à puce, et travaillent avec des émetteurs de cartes.

PAIEMENTS

Comme Visa et Mastercard et des organismes comme EMVco et Eurosmart, ils s'efforcent de garantir l'interopérabilité, la sécurité et la stabilité des technologies pour une industrie normalisée et durable.

BANQUES & DÉTAILLANTS

Partagent leurs exigences afin de s'assurer qu'ils ont le bon produit pour leurs clients.

CONSOMMATEURS

Utilisent de plus en plus la biométrie dans leur vie quotidienne* et recherchent le même niveau d'authentification pour les cartes de paiement, sans compromis sur la rapidité ou la commodité.

* Un utilisateur moyen de smartphone déverrouille son téléphone une centaine de fois par jour. Pour beaucoup, la biométrie a déjà remplacé le code PIN.

FINGERPRINTS