GEN KEY
Identity for all

GenKey BioHASH®

Une approche de la biométrie fondée sur le respect de la vie privée

GenKey Netherlands BV a son siège statutaire à Eindhoven, aux Pays-Bas et est enregistrée auprès de la Chambre de commerce néerlandaise sous le numéro 32132038.

Les informations présentées dans ce document sont susceptibles d'être modifiées sans préavis. GenKey n'assume aucune responsabilité pour les erreurs pouvant apparaître dans ce document. Ce document peut contenir des liens vers des sites Web tiers qui ne sont pas sous le contrôle de GenKey et GenKey n'est pas responsable du contenu de tout site lié ou de tout lien contenu dans un site lié, ou de toute modification ou mise à jour de ces sites.

Le logiciel GenKey BioHASH® est une information confidentielle et propriétaire de GenKey Netherlands BV. Aucune partie de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit - graphique, électronique ou mécanique, y compris la photocopie, l'enregistrement, l'enregistrement, le stockage ou la récupération d'informations - sans l'autorisation écrite de GenKey Netherlands BV

Contenu

A introduction

A1 Protection des informations biométriques

La biométrie est une approche très pratique et sécurisée pour vérifier l'identité des individus. Les empreintes digitales sont toujours disponible comme moyen d'identification et il est extrêmement difficile de prêter une empreinte digitale à un autre individu. La biométrie permet également de prouver qu'une personne est physiquement présente au moment de la vérification.

Tous les systèmes de vérification biométrique stockent des informations de référence biométriques sous forme d'images biométriques ou de modèles biométriques. Pendant la vérification, une mesure biométrique en direct est comparée aux informations de référence biométriques stockées et une décision est prise si le doigt utilisé pour générer les informations de référence stockées est le même que le doigt en direct proposé.

En raison de leur nature même, les informations biométriques sont sensibles et privées et doivent être traitées de manière hautement sécurisée et anonyme. Les informations de référence biométriques stockées peuvent être protégées à l'aide du chiffrement traditionnel, mais cela présente une vulnérabilité inhérente dans la mesure où les modèles doivent être déchiffrés pour effectuer une comparaison biométrique, ce qui les rend temporairement disponibles en texte clair pendant la comparaison et est alors vulnérable aux attaques. Il en va de même pour la mesure en direct: il est également important d'éviter que la mesure biométrique en direct ne soit compromise dans le processus de vérification.

Cette brochure décrit une approche fondamentalement différente du stockage et de la comparaison des informations biométriques. Nous appelons cette approche BioHASH® et sa philosophie et sa mise en œuvre sont basées sur le principe de «Privacy-by-Design».

A2 Gérer la variabilité biométrique

Une propriété fondamentale de la biométrie est la variabilité: une empreinte digitale (ou toute autre modalité biométrique) n'est jamais exactement la même que la précédente, même si elle provient du même doigt[1]. Les solutions biométriques classiques compensent cette variabilité au moment du match, en acceptant certaines tolérances sur les mesures. BioHASH® de GenKey est une approche radicalement différente de la biométrie en ce qu'elle génère un code reproductible et stable à partir des différentes biométries.

- Ce code BioHASH® stable peut être utilisé de différentes manières innovantes, permettant à la biométrie de devenir une partie intégrante de nombreux protocoles de sécurité. Les nombreux cas d'utilisation possibles sont décrits au chapitre B.
- L'application la plus fondamentale est que le code biométrique stable reproductible peut être protégé par hachage, conformément à la norme ISO / IEC 24745 pour la

[1]Avec les empreintes digitales, cette variabilité peut être causée par la façon dont vous placez votre doigt sur le scanner, les conditions environnementales telles que la température et l'humidité, et par la quantité de pression appliquée sur le capteur. Très souvent, différents capteurs sont utilisés pour l'inscription et la vérification.

protection des informations biométriques, offrant des avantages pour le stockage, la vérification et l'authentification sécurisés. Ceci est décrit plus en détail au chapitre C.

BioHASH® a réussi à relever le défi de dériver un code stable à partir d'entrées biométriques en constante évolution. Cela a été rendu possible en empruntant fortement aux techniques de traitement du signal telles que l'extraction de composants stables, la réduction du bruit, la correction des erreurs, etc. Le code stable généré par BioHASH® ou la valeur de hachage du code peut également être utilisé comme variable d'entrée dans des opérations cryptographiques, comme un code PIN, et même dans des protocoles client-serveur standardisés. Une liste des options de cas d'utilisation est décrite dans la section suivante.

BioHASH®n'est pas seulement un exercice académique. Il est déjà mis en pratique avec des millions de cartes d'identité émises et des milliers de transactions chaque jour, comme décrit au point B5.

B Cas d'utilisation BioHASH®

Dans cette section, divers exemples d'application de BioHASH® sont répertoriés, avec des cas d'utilisation allant des plus simples aux plus sophistiqués.

B1 Protection des informations biométriques

BioHASH® protège les informations biométriques de la même manière que les codes PIN et les mots de passe sont protégés en ce qu'un modèle BioHASH® est essentiellement le hachage cryptographique des informations biométriques représentées comme un code stable reproductible. Parce que BioHASH® est une approche sans clé, il n'est pas nécessaire de stocker et de gérer les clés, comme l'utilisation de certificats dans une infrastructure PKI.

Au niveau du processus, l'utilisation de BioHASH® dans une application biométrique est identique à l'utilisation d'une solution biométrique régulière non protégée: il y a enrôlement, stockage et vérification. La capture biométrique est transformée en un code BioHASH® et stockée sur une carte, en ligne ou dans une base de données. Pour une vérification biométrique, une empreinte biométrique en direct est capturée, hachée et comparée au code BioHASH® stocké dans le domaine haché, encore une fois très similaire à la façon dont les codes PIN et les mots de passe sont vérifiés. Le chapitre C décrit ce cas d'utilisation plus en détail.

B2 Le modèle petit et sécurisé permet des supports de stockage à faible coût

La taille d'un modèle BioHASH® peut être aussi petite que quelques centaines d'octets. Nous appelons ce format BioHASH®-C (pour Classic). Cela permet de stocker les informations dans des codes-barres 2D standard qui peuvent être imprimés sur du papier ou des cartes.

Une catégorie spéciale qui peut bénéficier de la sécurité intrinsèque des modèles stockés est celle où BioHASH® est imprimé sur des documents papier, comme les billets d'entrée, les cartes d'embarquement ou les incrustations Visa dans les passeports. Pour ces applications, il n'existe aucune alternative biométrique connue qui soit aussi flexible, privée et rentable. Une fois que vous avez capturé les données biométriques, tout ce dont vous avez besoin est une imprimante standard.

Lors de la vérification, le code-barres est scanné et le modèle BioHASH® est comparé à une mesure en direct de l'empreinte digitale.

Pour les applications plus exigeantes, des modèles légèrement plus grands peuvent être utilisés, de quelques Koctets. Ceux-ci peuvent être stockés dans la mémoire intégrée des cartes d'identité sans contact à faible coût et ils peuvent être personnalisés (biographies, photos) à l'aide d'imprimantes à cartes standard. Des fonctionnalités de sécurité supplémentaires (comme le numéro de carte d'identité ou les informations personnelles) peuvent être incluses dans le calcul du hachage et stockées dans le cadre du modèle BioHASH®. Cela protège également ces informations supplémentaires contre la falsification.

Les modèles plus grands, que nous appelons BioHASH®-D (pour Dual Layer), sont également la base des protocoles de vérification biométrique Client / Serveur entièrement privés décrits en B7, et pour la création de clés symétriques ou de paires de clés

asymétriques. Les clés secrètes symétriques et privées ne sont jamais stockées, mais régénérées à la volée à partir de la biométrie en direct uniquement lorsqu'une vérification biométrique est effectuée.

B3 BioHASH® pour générer un code PIN à partir d'un doigt

Le code stable qui est reproduit chaque fois qu'une vérification réussie par rapport à un modèle BioHASH® est effectuée, peut être utilisé comme code PIN biométrique. Il peut être utilisé à la place ou être combiné avec un code PIN normal pour, par exemple, authentifier un transfert d'argent à partir d'un téléphone mobile. Il peut également être utilisé pour les personnes qui ont tendance à oublier leur code PIN ou les personnes qui ne sont pas habituées aux codes PIN en général. Pour ce cas d'utilisation, nous recommandons d'utiliser BioHASH®-D. La longueur effective du code PIN pris en charge pour un seul doigt est de 5 chiffres, typique pour la plupart des applications de type bancaire. Des codes plus longs peuvent être pris en charge lorsque deux doigts sont utilisés.

B4 BioHASH® comme clé de cryptage

Une légère extension du concept d'utilisation de BioHASH® comme code PIN consiste à l'utiliser comme clé de cryptage. Cela permet de crypter les données personnelles avec une clé dérivée de ces données personnelles (auto-cryptage). Cela permet des conceptions de systèmes beaucoup plus simples pour protéger les informations (biométriques) qui n'ont pas besoin de s'appuyer sur des clés externes, qui sont traditionnellement gérées avec des certificats et des infrastructures PKI. Une opportunité évidente d'exploiter cela est dans la biométrie multimodale, où les modèles conventionnels de l'une des modalités peuvent être protégés par un cryptage biométrique basé sur une autre modalité. BioHASH®-C et BioHASH®-D prennent en charge ce cas d'utilisation.

B5 Une preuve de présence biométrique

Lorsqu'il y a une vérification réussie d'une personne par rapport à un code BioHASH®, exactement le même code stable est généré. Cela permet à BioHASH® de générer une preuve de présence en utilisant ce code biométrique stable pour générer une signature sur le résumé d'un document. Étant donné que la signature correcte ne peut être générée qu'après une vérification biométrique réussie, une telle signature garantit la présence de la personne. Pour ce cas d'utilisation, nous recommandons d'utiliser BioHASH®-D, bien que, comme le montre l'exemple ci-dessous, BioHASH®-C peut également être utilisé, mais pour des cas légèrement moins exigeants.

Un cas d'utilisation pratique

Au Ghana, la NHIA (National Healthcare Insurance Authority) s'est engagée avec GenKey pour lutter contre la fraude en émettant des cartes d'identité biométriques pour ses clients utilisant BioHASH®. Le premier objectif était de s'assurer que les membres qui détiennent des cartes d'assurance maladie s'identifient biométriquement par rapport à cette carte, afin qu'une carte d'assurance ne puisse pas être utilisée abusivement par d'autres personnes. Si un patient assuré visite un établissement de santé, une vérification réussie du patient par rapport à sa carte générera également une preuve de présence sous la forme d'un CVR (Code de vérification des réclamations). Ce code comprend des références à

l'emplacement du fournisseur de soins de santé, l'heure et le jour du traitement et il prouve qu'il y a eu une vérification biométrique réussie. Le CVR est copié manuellement sur le formulaire de réclamation qui est soumis à l'assureur, qui peut vérifier indépendamment la validité du CVR. Cela résout le problème des réclamations fantômes de certains établissements de santé qui ont déposé des réclamations pour des patients qu'ils n'avaient jamais traités. C'est pourquoi la devise de Genkey pour ses activités de soins de santé est:

«Moins de fraude = plus de soins».

À l'heure actuelle, ce programme compte environ 17,5 millions de participants actifs. Des programmes similaires sont également en cours d'exécution pour le Fonds national d'assurance des hôpitaux du Kenya, avec l'objectif d'enregistrer 4 millions de personnes.

B6 BioHASH® pour toutes les modalités

Bien que les empreintes digitales aient été largement utilisées à titre d'exemple et constituent actuellement la modalité avec le plus grand déploiement, BioHASH® est très bien adapté à d'autres modalités biométriques telles que la veine, l'iris, la voix et le visage. Le principe de base reste le même partout. Tout d'abord, la capture biométrique brute est transformée en un code BioHASH® qui peut être utilisé dans l'une des applications ci-dessus.

B7 BioHASH® pour une utilisation dans les protocoles cryptographiques

Cette brochure donne quelques exemples d'utilisation de BioHASH®. Tous ces exemples jusqu'à présent concernent, sous une forme ou une autre, une vérification locale. Il existe cependant de nombreux moyens flexibles d'incorporer la biométrie dans les protocoles cryptographiques rendus possibles par le code stable et reproductible représentant la biométrie. Un exemple est l'authentification biométrique entièrement privée vers un serveur (éventuellement non authentifié). Avec BioHASH®-D, il est possible de dériver une paire de clés publique-privée à partir d'une biométrie. En envoyant la clé publique à un serveur et en dérivant la clé privée correspondante sur le client à partir d'une mesure biométrique en direct, des protocoles d'authentification de clé publique-privée standard peuvent être utilisés pour effectuer une authentification biométrique, donnant au serveur la preuve que la personne correspondant à son public la clé est physiquement présente. Ces protocoles de clé publique-privée normalisés sont bien compris et examinés car ils sont couramment utilisés pour authentifier les ordinateurs les uns auprès des autres. Cette approche de l'authentification biométrique vers un serveur hérite automatiquement de toutes les propriétés de ces protocoles standardisés pour éviter les fuites d'informations lorsque les serveurs s'avèrent non fiables. Pour ce cas d'utilisation, BioHASH®-D est requis.

B8 Identités auto-souveraines

Les identités auto-souveraines (SSI) sont une nouvelle approche des identités en ligne. L'idée sous-jacente principale est que l'individu lui-même est en plein contrôle de tous ses attributs d'identité contenus dans un portefeuille électronique sur un appareil détenu et auquel il fait confiance. Ces attributs peuvent être émis et signés par une autorité de confiance telle qu'un gouvernement, une université ou une banque, ou ils peuvent être générés par l'individu lui-même. Lors de l'authentification vers un service, l'individu décide quelles informations sont

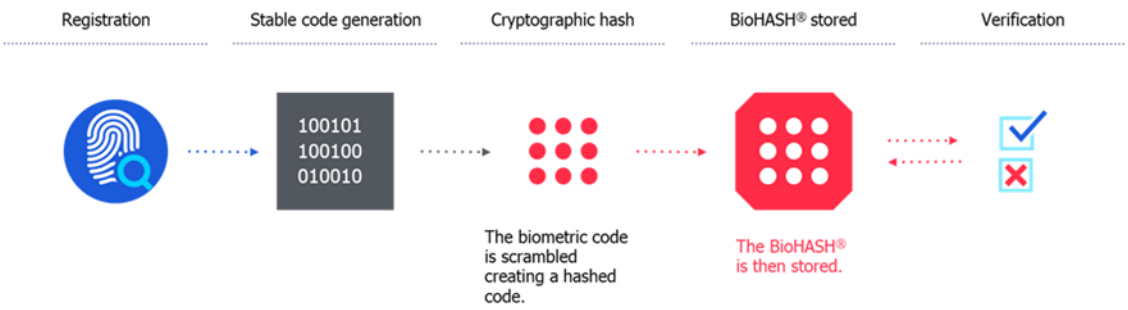
révélées au service et le portefeuille interagit ensuite avec le service, révélant la quantité minimale possible d'informations (souvent un seul bit). Un exemple d'initiative SSI est Sovrin (www.sovrin.org).

BioHASH® permet d'étendre les schémas SSI standardisés avec des attributs biométriques ajoutant une preuve irréfutable et totalement privée de présence personnelle au moment de l'interaction avec le service. Pour ces cas d'utilisation, BioHASH®-D est requis.

C Le cas le plus simple plus en détail: BioHASH® comme modèle biométrique sécurisé

C1 Codes stables et hachage biométrique

L'une des propriétés fondamentales d'une fonction de hachage cryptographique est le fait que même le plus petit changement en entrée générera un résultat haché complètement différent. Cette propriété est couramment utilisée pour la détection de falsification de documents ou de programmes informatiques, souvent en combinaison avec des signatures numériques pour détecter des changements même infimes. De plus, la technologie Blockchain s'appuie sur cette notion en formant une chaîne de hachage distribuée qui devient un registre qui ne peut pas être modifié ou falsifié. Une application plus basique pour utiliser les fonctions de hachage est de protéger les informations. Par exemple, le stockage des codes PIN et des mots de passe est protégé par des fonctions de hachage. En raison des propriétés des fonctions de hachage, lorsqu'il y a même une seule faute de frappe dans un mot de passe ou un code PIN, la vérification échoue. Lorsque vous protégez les codes PIN de cette façon, c'est bien sûr une propriété souhaitable, mais lors de l'application d'un hachage à la biométrie, la variabilité sur différents échantillons biométriques du même doigt crée un problème. La stabilité créée par BioHASH® résout ce problème et permet des propriétés qui ne sont pas facilement disponibles dans la biométrie conventionnelle, comme la révocabilité et la diversification entre plusieurs applications.



Fonctions cryptographiques à sens unique

Dans notre environnement quotidien, nous voyons de nombreuses situations qui sont «à sens unique» par nature, ce qui signifie qu'une transformation dans une direction est très courante, mais une transformation inverse est très rare, voire impossible. Si vous laissez tomber un verre et qu'il se brise en morceaux, il est très difficile de recréer le verre à partir des fragments, bien que vous puissiez envisager de faire fondre tous les morceaux pour recréer un verre à partir de la fonte. Dans d'autres cas, le sens inverse peut être complètement impossible: lorsqu'une cigarette est brûlée, il est physiquement impossible de recréer l'original à partir de la fumée et des cendres. Ce qui est cependant possible, c'est de recueillir de la fumée et / ou des cendres et d'effectuer une analyse, par exemple avec un spectromètre de masse.

De cette façon, vous pouvez caractériser la variété réelle de tabac utilisée, même si la cigarette n'existe plus.

En cryptographie, il existe une classe importante d'algorithmes qui ont la même fonctionnalité unidirectionnelle que celle décrite ci-dessus. Il est facile de convertir une entrée en sortie, mais pratiquement impossible de rétroconcevoir l'entrée en fonction de la sortie. La forme la plus connue et la plus utilisée est la fonction de hachage cryptographique. Ceci est couramment utilisé dans la protection des codes PIN et des mots de passe. BioHASH® utilise exactement cette approche et l'applique aux données biométriques, et dans l'analogie des cigarettes, seules les caractérisations sont stockées, jamais les données biométriques originales. C'est ce qui fait de BioHASH® une approche biométrique véritablement de deuxième génération, différente de toutes les biométries traditionnelles.

C2 BioHASH® protège les informations biométriques

Le code stable généré à partir de la biométrie par BioHASH® de GenKey peut être utilisé comme entrée pour une fonction de hachage cryptographique. Cela protège le code et toutes les informations sensibles et personnelles qui pourraient encore être présentes dans le code stable[2]. De plus, avant de hacher le code, des informations aléatoires supplémentaires sont ajoutées permettant de dériver différents codes de valeurs de hachage à partir de la même biométrique. Cela empêche le couplage de différentes bases de données (glissement de fonction) et permet la révocation / renouvellement pratiquement illimité des identifiants.

[2] Le code stable est déjà très abstrait et compressé à partir des images originales

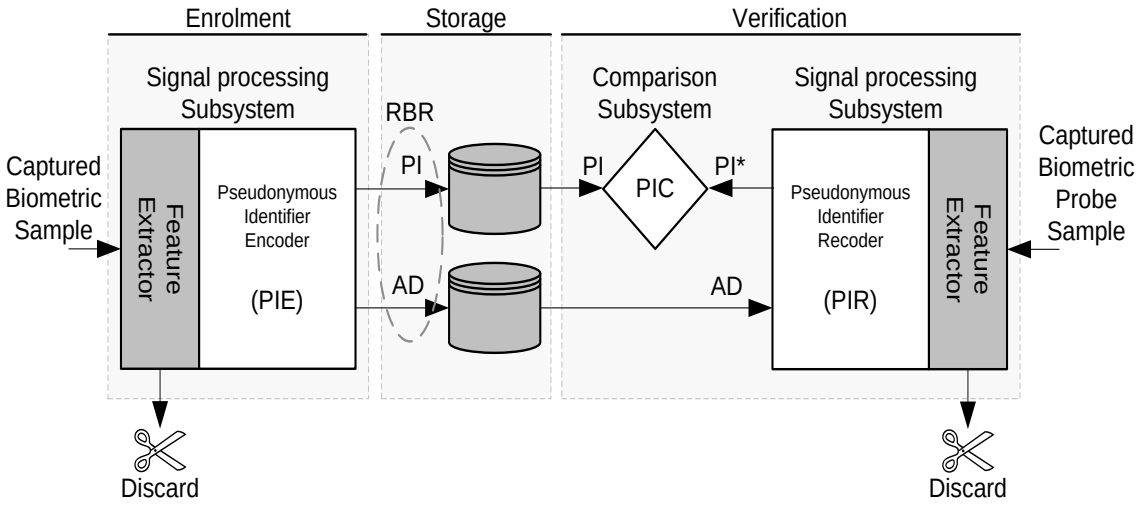
C3 BioHASH® est conforme à ISO / IEC 24745

La norme ISO / IEC 24745 pour la protection des informations biométriques fournit des conseils pour la protection des informations biométriques conformément aux exigences de confidentialité et de sécurité suivantes:

Irréversibilité et confidentialité: protéger les informations biométriques contre tout accès ou divulgation non autorisé pendant le stockage et la transmission.

Dissociabilité: empêche les références biométriques d'être reliables entre des applications ou des bases de données.

Renouvelabilité et révocabilité: permet de réémettre des références biométriques tout en révoquant la référence biométrique antérieure.



PI: Pseudonymous Identifier
AD: Auxiliary Data
PIC: Pseudonymous Identifier Comparator

Le lien entre cette image standard et la mise en œuvre réelle de BioHASH® est le suivant:

L'extracteur de fonctionnalités est un élément clé de BioHASH®, et avec PIE, il crée un modèle. PIE ajoute des éléments comme la graine aléatoire, un ID d'application et le salage, ainsi qu'une redondance pour permettre l'utilisation de codes de correction d'erreur plus tard dans le processus de vérification. Le modèle se compose de deux parties, le PI et l'AD. Aucun d'eux ne révèle aucune information sur les caractéristiques biométriques qui ont été utilisées pour les créer. Dans l'exemple le plus simple, PI et AD sont stockés ensemble[3]. Pendant la vérification, l'AD est combiné avec une sonde de vie, la correction d'erreur prend en charge les différences de placement des doigts, ce qui produit un PI * candidat. Cela crée une correspondance binaire avec le PI du modèle, si le modèle et la sonde proviennent du même doigt. Dans ce processus de génération de PI *, le caractère aléatoire introduit dans PIE s'annule.

[3]Il existe des applications qui peuvent bénéficier du stockage de PI et AD séparément, par exemple dans un modèle client / serveur. Voir la description sous B5.

D Considérations système

Il est évident que BioHASH® présente de nombreux avantages, donc une question naturelle à poser est de savoir quelles préoccupations posent l'utilisation de cette technologie. Ce chapitre les décrit en détail.

D1 Attaques biométriques Brute Force

La biométrie est une science statistique. Le point de fonctionnement choisi pour toute correspondance biométrique est toujours un compromis entre la probabilité que le système accepte un imposteur (FAR, False Accept Rate) et que le système rejette un véritable utilisateur (FRR, False Reject Rate). La plage typique de FAR se situe entre 1 sur 10 000 et 1 sur 100 000. Donc, si un attaquant est autorisé à exécuter une base de données de 100 000 entrées contre toute forme d'informations de référence biométriques protégées, il est très susceptible de trouver une biométrie fonctionnelle qui lui permettra de forcer l'entrée. Cela doit être évité au niveau du système. Voici des exemples de contre-mesures:

- Limitez le nombre de tentatives. Tout comme de nombreux systèmes basés sur PIN, les systèmes biométriques peuvent limiter le nombre de tentatives à 3.
- Augmentez la barrière contre l'entrée en force brute. Si un seul doigt peut atteindre un FAR de 1 sur 10 000, alors 2 doigts combinés pourraient théoriquement atteindre un FAR de 1 sur 100 000 000. En réalité, ce sera moins parce que les doigts d'un même individu ont des propriétés plus corrélées, mais en pratique, une barrière de 1 sur 10 000 000 peut être atteinte.
- Conception de système multifactorielle. Plutôt que de s'appuyer uniquement sur la biométrie, la combiner avec un jeton / téléphone mobile (quelque chose que vous avez) ou un code PIN ou un mot de passe (quelque chose que vous connaissez) peut renforcer considérablement la sécurité du système.

D2 Entropie biométrique limitée

On prétend que la biométrie est unique pour chaque individu, mais en réalité il y a une limite à la quantité de différenciation qui peut être distinguée par les systèmes biométriques, ou même par les observateurs humains. De nombreuses célébrités ont des sosies qui peuvent les remplacer ; de la même façon toute modalité biométrique individuelle a également des «doublons» dans la population mondiale. La quantité de différenciation est souvent appelée entropie. Cela présente une limite naturelle à la taille du nombre stable que BioHASH® peut dériver de chaque modalité. Malheureusement, les tailles typiques sont de l'ordre de 20 à 30 bits par mesure unique, certainement pas suffisantes pour être utilisées directement comme clé cryptographique où des longueurs d'au moins 128 bits sont requises[4]. Encore une fois, des contre-mesures sont nécessaires au niveau du système. Quelques exemples:

[4]Ces chiffres sont pour les empreintes digitales. Le visage et la voix sont légèrement pires, l'iris et la veine sont meilleurs, mais aucun d'eux n'est assez bon en soi pour atteindre une force jugée adéquate par les normes cryptographiques

- Biométrie multimodale et multi-doigts. Multi-modal fait référence au cas où différentes modalités sont combinées (par exemple empreinte digitale et fingervein), et multi-doigt fait référence au cas où 2 ou 4 doigts sont scannés.
- Modalités plus fortes. On sait que la veine et l'iris ont plus d'entropie que la voix, le visage ou les empreintes digitales.
- Empreintes digitales à échantillons multiples. En prenant deux échantillons ou plus du même doigt lors de l'inscription (ce qui est un événement unique) et en permettant une nouvelle tentative lors de la vérification (uniquement si la première tentative échoue), nous pouvons considérablement améliorer l'entropie, et donc les caractéristiques de correspondance et de sécurité de BioHASH®-C et BioHASH®-D.
- Salting. C'est le terme cryptographique lorsqu'un secret à entropie limitée (la biométrie) est amélioré par une longueur de clé beaucoup plus forte à partir d'un secret au niveau du système. Ensemble, ils créent une combinaison qui a une longueur de clé suffisante (principalement en raison du secret au niveau du système) et une grande variabilité (un secret différent est appliqué pour chaque individu en raison de la biométrie). La variabilité rend le secret salé beaucoup plus résistant aux attaques par rapport à l'alternative traditionnelle (cryptage symétrique) consistant à appliquer le même secret pour protéger les informations de tout le monde à l'échelle du système. GenKey utilise une implémentation WhiteBox pour le processus de salting.
- Différenciation et caractère aléatoire. Lorsqu'un modèle dérivé d'une propriété biométrique est toujours constant, il devient de plus en plus vulnérable à mesure que plusieurs échantillons sont produits. Lorsque le modèle contient un élément aléatoire pour chaque nouvelle instance, l'attaque du modèle devient beaucoup plus compliquée. C'est le cas à la fois pour BioHASH®-C et BioHASH®-D

D3 Contrer les attaques de retro-ingénierie.

La correspondance des modèles BioHASH® est généralement effectuée sur un appareil ou un serveur de vérification biométrique. Quel que soit le niveau de sécurité du modèle, si un attaquant peut obtenir la mesure en direct lorsqu'un utilisateur essaie de vérifier, la biométrie de cet utilisateur aura été compromise. Ainsi, au niveau du système et de l'appareil, des contre-mesures sont nécessaires, telles que:

- Blindage de certains logiciels critiques. Sur les appareils mobiles, cela se fait souvent dans TrustZone d'ARM, sur un PC, un TPM (Trusted Platform Module) peut être utilisé, et pour les serveurs, il existe un contrôle d'accès, TXT (Trusted eXecution Technology) et des technologies similaires.
- La protection contre les logiciels malveillants, les chevaux de Troie, etc. doit faire partie de chaque appareil et environnement système.
- Mesures dédiées contre a retro-ingénierie, l'émulation au moment de l'exécution et le débogage pour le SDK principal qui effectue le traitement biométrique. Genkey utilise une bibliothèque externe d'une entreprise de sécurité réputée pour exécuter cette fonction.

Genkey a été l'un des inventeurs de la protection des informations biométriques à l'aide de fonctions de hachage et possède un certain nombre de brevets et de nombreuses années d'expérience dans la conception de solutions biométriques bien équilibrées au niveau du système, et les systèmes résultants ont fait leurs preuves dans les déploiements de masse.

E Sommaire et conclusion

La possibilité de dériver un code stable à partir d'une biométrie en constante évolution ouvre de nombreuses applications. Celles-ci vont de la norme éprouvée sur le terrain et normalisée (ISO / CEI 24745) à la spéculation, comme l'utilisation d'identités biométriques dans un environnement SSI / Blockchain, où personne ne peut actuellement prédire où se situe le point idéal ultime. Cependant, il est certain que le déploiement de ces technologies peut être effectué au mieux par des personnes ayant des années d'expérience dans le type de considérations de niveau système pertinentes pour ce domaine. Veuillez donc consulter nos experts lorsque vous avez une idée d'application qui pourrait bénéficier de BioHASH®.

À propos de GenKey

Nous sommes experts en biométrie. Nous aidons des millions de personnes en Afrique et dans d'autres marchés émergents à identifier leur identité. En collaboration avec des partenaires, nous proposons des programmes d'identité biométrique à grande échelle, avec une vaste expérience des élections nationales et des soins de santé.

GenKey a ses racines dans la technologie biométrique de privacy-by-design. Notre approche unique de stockage et de comparaison des informations biométriques a évolué d'une proposition académique à un état mature qui est applicable partout où la confidentialité et la sécurité des données biométriques des utilisateurs finaux sont importantes. La technologie est protégée par plus de 10 brevets.

Identité pour tous

info@genkey.com

www.genkey.com