Garantir la sécurité de l'authentification mobile

COMMENT RELEVER LES PRINCIPAUX DÉFIS ET CRÉER DES SOLUTIONS D'AUTHENTIFICATION ROBUSTES POUR LES CONSOMMATEURS

Les solutions d'authentification mobile sont parmi les méthodes les plus sûres pour mettre en œuvre l'authentification multifacteur (MFA), qui permet d'ajouter une couche de protection éprouvée aux comptes et aux services en ligne des consommateurs. Elles sont également pratiques pour les utilisateurs, car elles se basent sur un appareil que la plupart des gens tiennent à portée de main.

Cependant, les méthodes d'authentification mobile et de signature des transactions évoluent rapidement. Il existe une vaste gamme de solutions sur le marché. L'une des méthodes les plus courantes consiste à utiliser un code sécurisé, communément appelé mot de passe à usage unique (OTP), envoyé par SMS aux téléphones mobiles des clients. D'autres solutions font appel aux technologies biométriques, comme la reconnaissance faciale ou des empreintes digitales.

Malheureusement, bon nombre de ces solutions présentent des failles de sécurité majeures. En effet, des analyses récentes montrent que la plupart des applications d'authentification mobile peuvent être victimes de logiciels malveillants. Les solutions qui se servent des SMS sont particulièrement vulnérables. Les SIM-swappers, par exemple, redirigent les numéros de téléphone des victimes sur leurs propres appareils et interceptent ainsi les messages privés. Même des services de messageries légitimes peuvent être utilisés pour rediriger les SMS des utilisateurs et accéder à leurs comptes de cette manière.

Que peuvent faire les entreprises pour se protéger et protéger leurs clients ? Dans ce livre blanc, nous passerons en revue les enjeux et expliquerons les facteurs qui rendent si difficile la sécurisation des systèmes d'authentification mobile. Ensuite, nous présenterons les contrôles et les protocoles qui existent pour élaborer des solutions sécurisées, transparentes et évolutives.

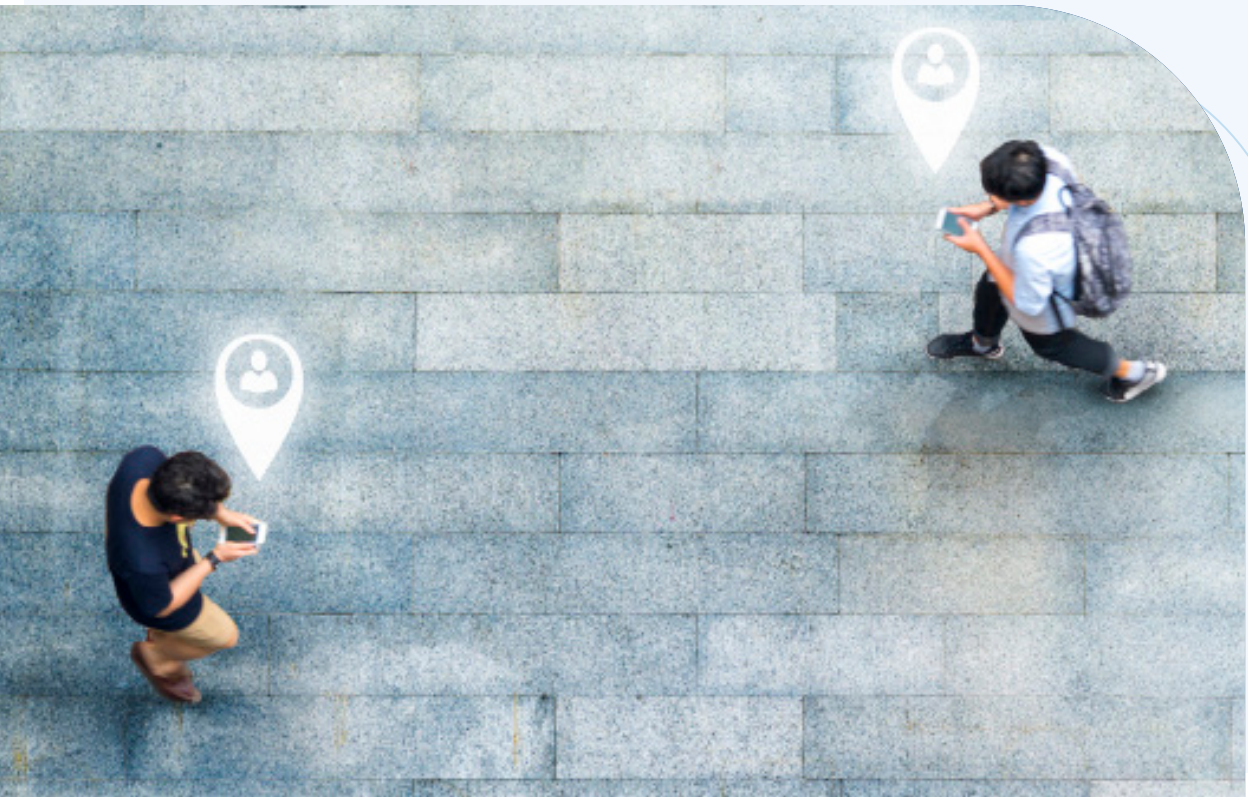
Les enjeux

Les enjeux de la sécurité de l'authentification mobile n'ont jamais été aussi élevés. Alors que le monde dépend de plus en plus du numérique, le volume d'attaques atteint de nouveaux records : en 2021, il y avait une cyberattaque toutes les 39 secondes. Le coût de la cybercriminalité augmente aussi de façon exponentielle. Elle a coûté aux organisations 1 000 milliards de dollars en 2020 et devrait dépasser les 10 000 milliards de dollars par an d'ici 2025.

Le vol d'identifiants reste la technique de prédilection des attaquants qui veulent s'infiltrer dans une organisation. Selon les estimations, 61 % de toutes les attaques exploiteraient des identifiants volés. Au cours d'une attaque importante menée en 2020, les attaquants ont construit un réseau de 16 000 appareils mobiles virtuels, puis ont intercepté des OTP par SMS pour extraire des millions de dollars d'applications bancaires mobiles en quelques jours.

Au printemps 2021, des pirates ont dérobé des cryptomonnaies sur environ 6 000 comptes Coinbase en exploitant une faille d'authentification multifacteur pour récupérer des informations sur les comptes des utilisateurs en introduisant un mot de passe à usage unique envoyé par SMS.

Ces dommages sont regrettables – d'autant plus qu'ils auraient pu être évités si des techniques de sécurité d'authentification plus robustes avaient été en place.



Les bases de la sécurité de l'authentification mobile

L'authentification mobile permet aux utilisateurs de tirer parti de certaines fonctionnalités existantes de leur appareil mobile pour vérifier leur identité, afin d'accéder à une application ou d'effectuer une transaction. La possibilité de se servir des smartphones, des appareils d'authentification faciles à utiliser et toujours à portée de main, présente un attrait évident. Malheureusement, la sécurisation du processus d'authentification mobile n'est pas une tâche facile.

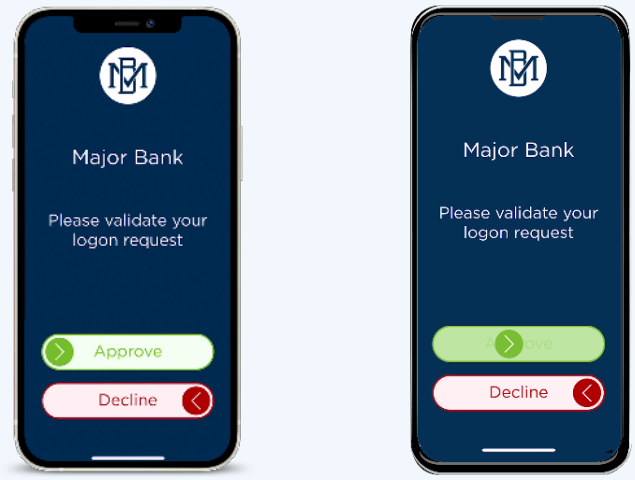
L'Open Web Application Security Project (OWASP), une fondation à but non lucratif qui travaille à améliorer la sécurité des logiciels, a établi des normes de sécurité de base. Cependant, contrairement aux applications web, les applications mobiles offrent aux développeurs beaucoup plus de possibilités au niveau des emplacements de stockage des données et de l'utilisation des fonctionnalités de sécurité intégrées des appareils pour authentifier leurs utilisateurs. Par conséquent, des choix de conception en apparence anodins peuvent avoir un impact majeur sur la sécurité globale de la solution.

LES MÉRITES DE L'AUTHENTIFICATION PUSH

Pour la plupart des gens, la vérification par SMS est devenue omniprésente. Les institutions financières interrogées par HID Global en 2021 la citent comme leur principale méthode d'authentification, et selon le Ponemon Institute, environ un tiers des utilisateurs mobiles l'utilisent – malgré les risques de sécurité majeurs qui y sont associés.

Par contre, l'authentification par notification push offre aux entreprises une combinaison plus puissante de sécurité, de flexibilité et d'ergonomie. La technologie push utilise des techniques cryptographiques pour lier un appareil spécifique à l'identité de son propriétaire, rendant impossible l'usurpation d'identité d'une personne sans accès physique à l'appareil. Elle est ainsi plus sûre que l'authentification par SMS, car les fournisseurs de services n'envoient pas d'informations sensibles aux appareils des clients via un réseau non sécurisé. Les clés peuvent être encore mieux protégées lorsqu'elles sont associées à l'appareil via son dispositif de sécurité, ce que nous verrons plus loin.

De plus, l'expérience utilisateur est plus simple qu'avec les SMS. Lorsqu'une notification push apparaît à l'écran, l'utilisateur n'a qu'à appuyer sur « Approuver » ou « Refuser » plutôt que de devoir saisir un mot de passe à usage unique reçu par SMS.



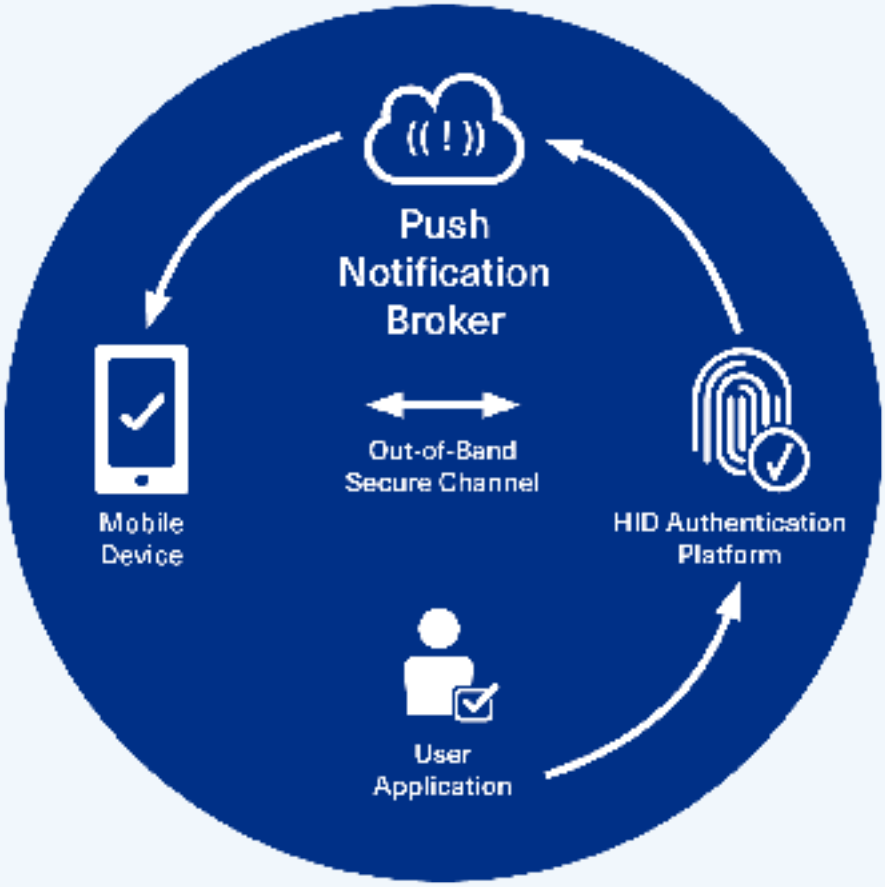
Exemple de solution d'authentification par balayage HID Approve personnalisée

SÉCURISER L'ENSEMBLE DU PARCOURS D'AUTHENTIFICATION

Les utilisateurs ne voient généralement qu'une très petite partie du processus d'authentification, car l'essentiel se déroule en arrière-plan. Le cycle de vie complet de l'authentification mobile comprend :

- Enregistrement (et reconnaissance) de l'appareil de l'utilisateur
- Provisionnement d'identifiants sécurisés à l'utilisateur
- Protection des identifiants utilisateur
- Sécurisation des communications entre l'utilisateur, l'application et les serveurs back-end
- Protection des requêtes de données sensibles effectuées pendant l'exécution de l'application de votre entreprise
- Maintien de la sécurité tout au long du cycle de vie du client
- Prévention des attaques par force brute

Chaque étape présente des défis. Dans la section suivante, nous examinons ces défis de plus près et passons en revue des solutions spécifiques pour y faire face.



Principaux défis en matière de sécurité de l'authentification mobile

De nombreux facteurs compliquent la sécurité de l'authentification mobile. Il s'agit à la fois de sélectionner les techniques les plus efficaces et de les intégrer aux systèmes de sécurité de votre entreprise. Dans les pages suivantes, nous passons en revue les huit principaux défis en la matière et présentons les meilleures solutions pour protéger les données et empêcher les attaques.

1. AUTHENTIFICATION DES APPAREILS DES UTILISATEURS

Le défi : L'une des meilleures façons de confirmer l'identité numérique d'une personne est de détecter si elle utilise bien son propre appareil. Sinon, des attaquants pourraient usurper son identité en transférant ses données dans un clone réel ou virtuel, difficile à distinguer de l'appareil authentique.

La solution : La technologie anti-clonage garantit que toute personne qui tenterait d'accéder aux systèmes via un appareil cloné sera bloquée.

Les techniques anti-clonage les plus sûres reposent sur le dispositif de sécurité fourni avec pratiquement tous les smartphones modernes. Sous iOS, il s'agit de Secure Enclave. Pour les appareils Android, cela s'appelle l'environnement d'exécution de confiance (« Trusted Execution Environment » ou « TEE »). Les ordinateurs portables disposent d'un dispositif similaire, connu comme le « Trusted Platform Module » (TPM). Quel que soit son nom, le dispositif de sécurité permet aux solutions d'authentification d'exploiter pleinement les mesures de sécurité matérielle intégrées.

Mais ce n'est pas tout. Les solutions d'authentification les plus robustes prévoient plusieurs couches de protection par chiffrement pour bloquer les clones potentiels, en sécurisant les clés individuelles avec une clé d'appareil unique générée lors du processus de provisionnement initial. Même si cette clé d'appareil était compromise, l'attaquant ne pourrait accéder à aucune autre clé, ni faire passer un clone pour l'appareil en question.

2. PROVISIONNEMENT DES APPAREILS DES UTILISATEURS

Le défi : Le processus de provisionnement des identités permet à votre organisation de gérer les identités des utilisateurs et d'attribuer un identifiant à leurs appareils mobiles. Il est impératif de le sécuriser et de le protéger des attaques.

La solution : Certaines solutions d'authentification mobile font appel à la cryptographie à clé publique, une technologie qui repose sur l'association mathématique d'un couple de clés, l'une privée et l'autre publique, pour activer les appareils des utilisateurs. La clé privée, générée par l'appareil de l'utilisateur, est considérée comme secrète et ne quitte jamais l'appareil, ce qui réduit le risque que les identifiants soient compromis. C'est une solution efficace pour les appareils d'authentification mobiles qui peuvent échanger directement avec le serveur d'authentification lors des requêtes d'authentification sans intervention manuelle de l'utilisateur (par exemple, pour les authentifications push).

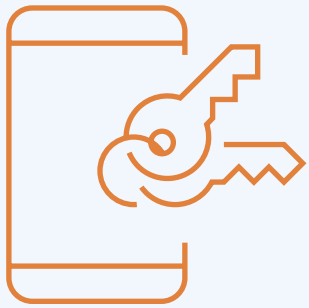
Mais pour les systèmes d'authentification qui impliquent une intervention manuelle (comme un mot de passe à usage unique), un échange de clé secrète entre l'appareil mobile et le serveur d'authentification est inévitable. La sécurisation de l'échange de la clé secrète entre le client et le serveur repose sur deux aspects :

1) L'authentification initiale de l'utilisateur, pour établir un canal sécurisé pour l'échange des secrets

2) Le canal sécurisé en lui-même

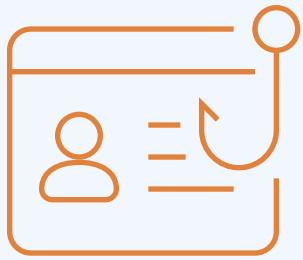
Les solutions les plus sûres garantissent une authentification initiale unique pour chaque utilisateur, utilisée une seule fois et qui expire immédiatement après l'enregistrement. En outre, elles permettent aux organisations de personnaliser des paramètres et des règles de sécurité spécifiques, comme la longueur et la composition alphanumérique du code d'authentification initial, mais aussi le nombre de tentatives autorisées en cas d'échec de l'authentification initiale.

Il y a aussi des considérations relatives aux politiques qui régissent les processus de provisionnement des identifiants. Les meilleures solutions d'authentification vous permettront de déterminer si vous souhaitez ou non émettre des identifiants pour d'anciens systèmes d'exploitation, des téléphones débridés ou des appareils dépourvus de dispositif de sécurité. Elles vous laisseront choisir le type de chiffrement à utiliser et faciliteront la configuration de ces paramètres, plutôt que de vous forcer à accepter les réglages prédéfinis par le fournisseur de la solution.



3. PROTECTION DES IDENTIFIANTS DES UTILISATEURS

Le défi : Les identifiants des utilisateurs sont vulnérables à plusieurs types d'attaques et au hameçonnage. Il est nécessaire de mettre en place des politiques robustes pour les protéger.



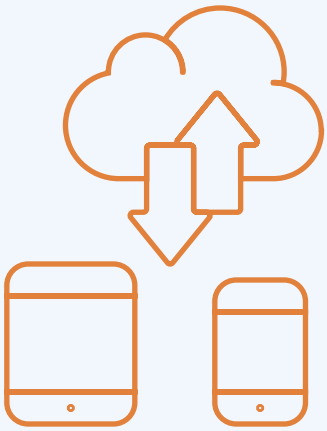
La solution : Les politiques des mots de passe diffèrent d'une entreprise à l'autre. Les meilleures solutions d'authentification mobile s'adaptent à ces différences, soit en déclenchant une notification push aussitôt après la saisie d'un mot de passe, soit en exigeant des utilisateurs qu'ils prennent d'abord des mesures supplémentaires pour confirmer leur identité, comme en saisissant le code PIN ou le mot de passe de leur appareil ou en présentant un marqueur biométrique.

De fait, la protection des identifiants des utilisateurs implique souvent de mener une réflexion poussée sur les aspects pratiques et la convivialité. Les mots de passe à 15 caractères peuvent être plus sûrs qu'un code PIN à quatre chiffres, mais ils sont aussi plus difficiles à retenir et fastidieux à introduire dans un téléphone portable. La biométrie présente un excellent mélange de sécurité et de commodité, et la plupart des appareils mobiles disposent désormais de capacités biométriques intégrées. Les meilleures solutions permettent aux entreprises de choisir si elles exploitent celles-ci et comment, de même que d'autres techniques.

4. SÉCURISATION DES COMMUNICATIONS

Le défi : Les données sensibles qui transitent par des canaux non sécurisés risquent d'être interceptées. La communication entre les utilisateurs, les solutions d'authentification mobile et les serveurs back-end doit donc être chiffrée.

La solution : Avant tout échange de messages, votre solution d'authentification mobile doit s'assurer qu'elle communique avec le bon serveur. L'épinglage de certificat permet de s'en assurer, en restreignant les certificats considérés comme valides pour ce serveur. Cela établit un lien de confiance explicite entre votre solution d'authentification et vos serveurs et réduit votre dépendance vis-à-vis d'organismes tiers.



Pour assurer la sécurité de la couche de transport, il est indispensable d'adopter le protocole TLS. La norme TLS 1.2 sécurise la couche de transport de manière à protéger chaque message échangé entre la solution d'authentification et le serveur, ainsi que toute notification envoyée à l'appareil mobile. Pour assurer la sécurité au niveau des messages, les informations à l'intérieur de ce tunnel sécurisé doivent également être chiffrées.

Les meilleures solutions d'authentification vont encore plus loin, notamment en n'exigeant pas l'envoi de données d'utilisateur sensibles dans les notifications push, mais en utilisant plutôt un canal privé et sécurisé entre l'application et le serveur pour récupérer le contexte de la demande. Cette méthode renforce la sécurité en limitant le potentiel d'exposition et d'intrusion.

5. BLOCAGE DES ATTAQUES EN TEMPS RÉEL

Le défi : Avec la hausse des vulnérabilités dites « zero-day », il est impératif que toutes les applications disposent de mécanismes de détection et de blocage des attaques en temps réel.

La solution : Runtime Application Self Protection, ou RASP, est un ensemble de technologies et de techniques de contrôle qui permettent de détecter, de bloquer et de neutraliser les attaques qui surviennent pendant l'exécution de l'application. Cela empêche notamment la rétro-conception et la modification non autorisée du code, sans nécessiter d'intervention humaine.

Les meilleures solutions de cette catégorie utilisent des défenses multicouches pour réduire la probabilité qu'un seul contrôle contourné n'aboutisse à une violation dangereuse. Ces défenses incluent :

- L'offuscation du code, qui rend le code source décompilé plus difficile à comprendre pour un être humain sans altérer l'exécution du programme.
- Les technologies de détection des tentatives de sabotage, comme l'ASLR, le SSP et les vérifications des fichiers de liste de propriétés (ou .plist checks), qui garantissent que l'application et son environnement n'ont pas été compromis ni altérés.
- La détection des débridages et des émulateurs, qui permet aux organisations de créer et de mettre en œuvre des politiques relatives aux types d'appareils considérés comme fiables ou non.

6. RATIONALISATION DE LA GESTION DU CYCLE DE VIE D'AUTHENTIFICATION

Le défi : Pour réduire le risque que les clés de chiffrement et les certificats délivrés aux appareils soient compromis, ceux-ci ont des cycles de vie limités dans le temps. Plus le cycle de vie est court, plus la clé est sûre. Bien entendu, des cycles de vie plus courts obligent aussi les organisations à adopter des plans de gestion et de renouvellement bien organisés, ainsi qu'à prévoir une solution qui n'oblige pas les utilisateurs à se réinscrire constamment au service.

La solution : Les meilleures solutions d'authentification permettent de configurer facilement la durée de vie d'une clé. Elles ont également un mécanisme par lequel le serveur peut renouveler les clés d'un appareil avant qu'elles n'expirent, sans intervention de l'utilisateur. Cela permet aux entreprises d'adhérer aux meilleures pratiques de sécurité sans perturber le service fourni à leurs clients.

HID

7. PRÉVENTION DES ATTAQUES PAR FORCE BRUTE

Le défi : Les attaques par force brute procèdent par essai et erreur pour déduire les informations de connexion et les clés de chiffrement. C'est une méthode à la fois simple et étonnamment efficace. Les chercheurs de l'entreprise de cybersécurité ESET ont détecté 55 milliards de nouvelles tentatives d'attaques par force brute entre mai et août 2021, soit plus du double des 27 milliards d'attaques détectées entre janvier et avril de la même année.

La solution : Les solutions d'authentification mobile s'appuient sur des techniques diverses pour contrer ce type d'attaque. Les solutions les plus robustes vous permettent de personnaliser les paramètres d'après vos besoins et vos politiques spécifiques.
Les techniques les plus efficaces sont notamment :

- Les blocages à retardement, qui imposent des délais croissants avant que les utilisateurs qui saisissent un code PIN ou un mot de passe incorrect puissent réessayer.
- Les blocages à compteur, qui rendent les mots de passe non valides après un certain nombre de tentatives infructueuses.
- Les blocages silencieux, qui ne fournissent aucun retour d'information à l'utilisateur qui saisit un code PIN ou un mot de passe incorrect, mais bloquent tout simplement son accès au système.

HID

Garantir une protection continue

Le défi : Les fournisseurs de sécurité promettent de protéger vos systèmes. Mais comment pouvez-vous vous assurer que leurs solutions seront efficaces et qu'elles suivront les évolutions rapides en matière de sécurité ?

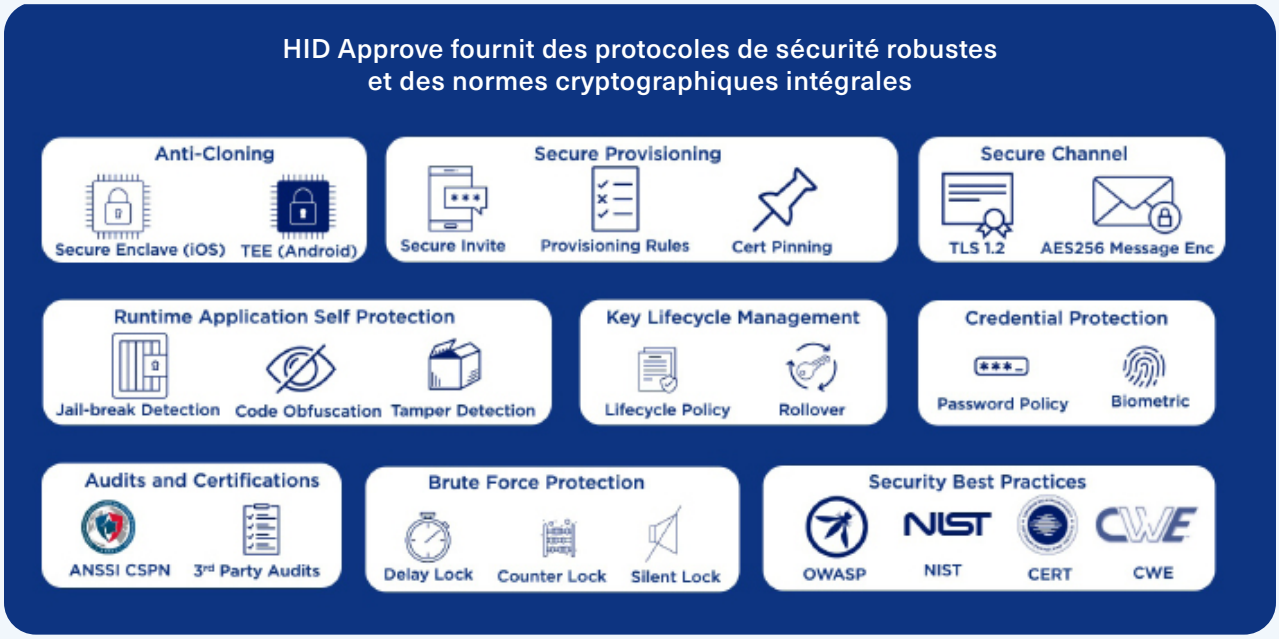
La solution : Les audits tiers et les examens de conformité des attestations – internes et externes – sont la façon la plus efficace de s'assurer de la stabilité et de la sécurité des solutions d'authentification. Les vérifications internes devraient évaluer la conformité de la solution à un ensemble de contrôles de sécurité basés sur la norme du secteur : l'Application Security Verification Standard (ASVS) de l'OWASP.

Quant aux audits de pénétration externes, comme la Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'ANSSI française (Agence nationale de la sécurité des systèmes d'information), ils devraient certifier la robustesse de la solution d'après une analyse de conformité et des tests d'intrusion **rigoureux.**

Créer des solutions d'authentification mobile sécurisées et évolutives

L'authentification multifacteur est valorisée à juste titre pour sa capacité à bloquer les attaques. Or de plus en plus, les solutions MFA en elles-mêmes sont prises pour cible par les pirates. Et vu les conséquences et les coûts potentiels de la moindre intrusion, il est clair que le moment est venu pour les entreprises de veiller sérieusement à la sécurité de leurs procédures d'authentification mobile.

La protection des procédures d'authentification mobile, de l'enregistrement des appareils des utilisateurs à la gestion des identifiants en passant par les audits de sécurité, n'est pas une tâche facile. Mais en faisant preuve de minutie et en utilisant des techniques qui exploitent toutes les fonctionnalités de sécurité des appareils, vous pourrez élaborer des solutions qui vous protégeront contre une panoplie de menaces toujours plus diverses.



VOUS AVEZ BESOIN D'AIDE POUR SÉCURISER VOS SYSTÈMES D'AUTHENTIFICATION MOBILE ?

- Consultez la page web Authentification et HID Approve
- Téléchargez le nouvel e-book HID Approve : Authentification push mobile et signature des transactions en toute simplicité
- Réservez une démonstration d'authentification avec l'un de nos experts directement dans le calendrier

hidglobal.com

Amérique du Nord : +1 512 776 9000 | Numéro gratuit : 1 800 237 7769
Europe, Moyen-Orient, Afrique : +44 1440 714 850
Asie-Pacifique : +852 3160 9800 | Amérique latine : +52 (55) 9171-1108
Pour plus de numéros de téléphone internationaux, cliquez ici

2022-04-12-iams-ensuring-mobile-authentication-security-wp-fr PLT-06608
Fait partie d'ASSA ABLOY