Livre blanc

Introduction aux passkeys

Comment l'authentification FIDO résistante au phishing améliore les expériences utilisateurs et prévient le piratage de comptes

Sommaire

Introduction

L'histoire des technologies retiendra sans doute l'adoption des passkeys, et des passkeys synchronisées en particulier, comme un point d'inflexion dans l'authentification web résistante au phishing et la transition plus large vers un modèle sans mot de passe.

Les passkeys liées au terminal ont fait leur apparition il y a quelques années, mais certains des aspects qui contribuent à une authentification forte (comme le fait qu'elles ne soient liées qu'à un seul terminal) ont limité leur adoption par le plus grand nombre.

En revanche, les passkeys synchronisées :

- peuvent être synchronisées sur une myriade de terminaux ;
- permettent la mise en œuvre de l'authentification multifacteur (MFA) en une seule étape.

Ces caractéristiques contribuent à la convivialité de l'expérience et devraient considérablement accroître l'attrait des passkeys synchronisées aux yeux du grand public.

Qui plus est, les passkeys renforcent de manière significative la sécurité des comptes pour la majorité des utilisateurs, ce qui réduit le piratage de comptes et évite aux utilisateurs et aux fournisseurs de services de subir diverses conséquences préjudiciables.

Si les passkeys ne constituent pas une solution d'authentification parfaite répondant à tous les besoins des utilisateurs dans toutes les situations, nous estimons qu'il s'agit néanmoins d'une alternative préférable aux mots de passe, viable et résistante au phishing. C'est pourquoi nous nous sommes donné pour mission de simplifier l'intégration des passkeys aux flux d'authentification pour les développeurs.

Pour encourager l'adoption des passkeys, ce document :

- passe en revue leurs avantages ;
- s'intéresse à leur fonctionnement ;
- explore différentes façons de les implémenter.

Les passkeys sont des identifiants FIDO détectables par les navigateurs ou hébergés dans des applications natives ou des clés de sécurité pour une authentification sans mot de passe. Basées sur les normes de la FIDO Alliance et du World Wide Web Consortium (W3C), les passkeys remplacent les mots de passe par des paires de clés cryptographiques.

Les passkeys se présentent sous deux formes :

- Les passkeys synchronisées, qui sont synchronisées sur les terminaux de l'utilisateur via un service cloud, tel que l'écosystème d'un système d'exploitation ou un gestionnaire de mots de passe
- Les passkeys liées à un terminal, qui ne quittent jamais le terminal ; elles peuvent être utilisées par des authentificateurs certifiés FIDO et des clés de sécurité, y compris celles ayant obtenu une certification de niveau de sécurité

En pratique, les passkeys synchronisées remplacent la combinaison des mots de passe et du MFA pour les comptes utilisateur standard, tandis que les passkeys liées à un terminal peuvent offrir une protection et une assurance renforcées.

La FIDO Alliance et Okta

Fondée en 2012 et lancée publiquement en 2013, la FIDO Alliance est une association sectorielle ouverte dont la mission consiste à développer et à promouvoir des normes d'authentification qui « contribuent à réduire la dépendance excessive aux mots de passe ».

À cette fin, l'association :

- développe des spécifications techniques qui définissent un ensemble ouvert, évolutif et interopérable de mécanismes réduisant la dépendance aux mots de passe pour l'authentification des utilisateurs ;
- dirige des programmes de certification pour favoriser une adoption mondiale réussie des spécifications ;
- soumet des spécifications techniques matures à des organismes de développement de normes reconnus pour une normalisation formelle.

Okta est un membre sponsor de la FIDO Alliance. (Pour consulter la liste complète des membres, cliquez ici.)

Comprendre la terminologie grâce à un bref historique des passkeys

La terminologie dans le domaine des passkeys a évolué et peut prêter à confusion. Voici un bref historique qui devrait vous aider à y voir plus clair.

En avril 2018, la norme d'authentification web du W3C a atteint le statut de candidat à la recommandation et FIDO2 a été officiellement lancé. Développé par la FIDO Alliance, FIDO2 spécifie un standard d'authentification web via une API JavaScript, communément appelé WebAuthn, ainsi que le protocole CTAP (Client-to-Authenticator Protocol) correspondant.

L'API JavaScript permet aux développeurs d'utiliser soit des clés physiques (appelées authentificateurs itinérants), soit du matériel sécurisé sur le terminal (appelé authentificateurs de plateforme). Ce dernier est souvent sécurisé par des capteurs biométriques permettant d'authentifier les utilisateurs sans mot de passe.

En faisant abstraction de l'emplacement où sont hébergées les clés publiques et privées, cet ensemble de spécifications a considérablement élargi la disponibilité des fonctionnalités d'authentification résistantes au phishing sur les terminaux modernes.

En mai 2022, les géants de la technologie Apple, Google et Microsoft ont annoncé qu'ils prévoyaient de développer FIDO2 en prenant en charge la sauvegarde des authentificateurs de plateforme grâce à un nouveau mécanisme de synchronisation. L'objectif de cet ensemble élargi de fonctionnalités est de simplifier le remplacement des mots de passe par des identifiants FIDO pour les sites web et les applications.

Même si le communiqué de presse comprenait une occurrence du terme « passkey », à l'époque :

- le terme « passkey » ne désignait que les identifiants FIDO multi-terminaux ;
- l'expression « identifiants FIDO multi-terminaux » était le terme privilégié.

Par la suite, le terme « passkey » en est venu à désigner les identifiants FIDO détectables de manière générale.

Toutefois, avec l'introduction généralisée des passkeys et leur adoption par des plateformes de premier plan, la FIDO Alliance s'est arrêtée sur le terme « passkeys », qui englobe désormais à la fois les passkeys synchronisées et les passkeys liées à un terminal. Le terme « identifiants multi-terminaux » a alors été abandonné.

Les avantages des passkeys

L'adoption massive des passkeys par les utilisateurs représenterait un grand pas en avant dans la lutte contre le phishing, le piratage de comptes et autres menaces ciblant l'identité.

Si l'idée reçue est qu'une authentification plus sécurisée n'est possible qu'en sacrifiant l'expérience utilisateur, les passkeys ont le potentiel de renforcer la sécurité tout en optimisant les expériences utilisateurs grâce à la simplification et à l'accélération des flux d'authentification.

Les passkeys sont plus sécurisées que les mots de passe (et les techniques MFA traditionnelles)

Ce n'est un secret pour personne : les mots de passe sont une piètre solution au problème de l'authentification des utilisateurs. Ils sont même devenus matière à plaisanter — pour preuve, ces trois comics sur le site xkcd : Password Reuse, Password Strength et Encryptic.

Ce qui était au départ un simple espace de connexion renseigné par des humains a radicalement changé au fil des années.

- À mesure que les cybercriminels sont passés maîtres dans l'art de deviner des mots de passe faibles et de tirer parti de la réutilisation massive des mots de passe, les exigences en matière de complexité ont évolué, conduisant à des mots de passe toujours plus longs avec des caractères spéciaux et des combinaisons de minuscules, majuscules et chiffres.
- Les utilisateurs ont eu à gérer des mots de passe plus complexes et toujours plus nombreux, ce qui a favorisé l'adoption de gestionnaires de mots de passe (intégrés à un navigateur ou via une application distincte).
- Le phishing a pris de l'ampleur et d'énormes dépôts de mots de passe sont apparus en ligne. Le MFA s'est alors imposé comme une défense efficace contre le piratage de comptes.
- Aujourd'hui, de nombreuses techniques MFA plus anciennes sont ciblées par des menaces, car les cybercriminels trouvent des moyens évolutifs et économiques de contourner cette défense.
- Au fil du temps, mais principalement en arrière-plan, les systèmes de gestion des identités collaborateurs et clients ont introduit des couches de sécurité pour lutter contre un large éventail de cyberattaques automatisées, qui coûtent de l'argent aux entreprises et menacent la confidentialité des clients.

Bon nombre de ces changements ont dégradé l'expérience utilisateur en ajoutant des points de friction à des actions quotidiennes telles que l'inscription à un service ou la connexion à un compte.

Heureusement, les passkeys offrent une alternative aux mots de passe résistante au phishing, qui fournit également un deuxième facteur d'authentification de manière implicite.

Problèmes associés aux mots de passe

Basé sur une étude menée auprès de 21 512 consommateurs dans 14 pays, le rapport Okta Customer Identity Trends Report révèle que :

- 65 % des personnes interrogées se sentent dépassées par le nombre de noms d'utilisateur et de mots de passe qu'elles doivent gérer.
- 33 % indiquent ressentir de la frustration lorsqu'elles doivent créer un mot de passe respectant un certain nombre de critères.
- 25 % mentionnent ressentir de la frustration lorsqu'elles doivent créer un nouveau mot de passe pour chaque service en ligne.

Les passkeys sont résistantes au phishing

Pour les marques B2C (business-to-consumer), le remplacement des mots de passe par les normes FIDO signifie que les attaques automatisées et intersites ciblant les mots de passe, comme le password spraying ou le password stuffing, n'aboutiront pas lorsqu'elles visent leurs sites web. En outre, grâce à l'utilisation de la cryptographie à clé publique par FIDO, les entreprises n'ont besoin de stocker que la clé publique d'un utilisateur, qui a une valeur négligeable pour les cybercriminels. La clé privée de l'utilisateur est stockée de manière sécurisée sur son terminal. Elle reste sur les terminaux de confiance de l'utilisateur, ce qui permet une synchronisation parfaite au sein de l'écosystème du système d'exploitation ou via un service tiers fiable. La synchronisation des passkeys est chiffrée de bout en bout, ce qui protège les informations sensibles tout au long du processus.

En plus de réduire les risques et l'exposition des entreprises, une telle résilience profite également aux utilisateurs. Ceux qui choisissent d'utiliser des passkeys sont bien moins susceptibles d'être victimes d'un piratage de comptes et de ses répercussions, qu'il s'agisse de désagréments mineurs, d'une atteinte à la vie privée ou même d'une usurpation d'identité.

Les passkeys peuvent fournir implicitement un MFA fort

L'authentification multifacteur (MFA) requiert au moins deux facteurs d'authentification. Par exemple :

- Un facteur de connaissance → un élément que vous connaissez, comme un mot de passe, un code PIN ou une question de sécurité
- Un facteur de possession → un élément que vous possédez, tel qu'un terminal géré
- Un facteur d'inhérence → une caractéristique qui vous est propre, par exemple votre empreinte digitale

Étant donné que les passkeys sont conservées sur les terminaux d'un utilisateur (un facteur de possession) et que, lorsqu'une vérification est requise, elles peuvent uniquement être appliquées par l'utilisateur via la biométrie, un code de sécurité ou une autre technique conforme à FIDO (un facteur d'inhérence ou de connaissance), elles satisfont implicitement le principe fondamental du MFA.

Le MFA fourni par les passkeys fait partie des plus forts disponibles. Il représente un grand bond en avant par rapport à la protection offerte par les magic links et les codes à usage unique (OTP), qui restent monnaie courante à l'heure actuelle.

Pour de nombreuses entreprises orientées clients, les avantages en termes de sécurité suffisent à justifier l'implémentation de la prise en charge des passkeys, même si ce n'est pas le seul facteur à prendre en compte.

Les passkeys pour les cas d'usage à niveau d'assurance modéré

Toutes les passkeys partagent plusieurs propriétés de sécurité communes, sont hautement résistantes au phishing et utilisent des paires de clés uniques pour appliquer une authentification forte. Il existe toutefois des différences importantes entre les passkeys synchronisées et les passkeys liées à un terminal, ce qui affecte leur adéquation à divers cas d'usage.

Pour aider les entreprises à prendre des décisions éclairées, notamment en ce qui concerne les niveaux d'assurance relatifs à l'authentification (AAL) du NIST (National Institute of Standards and Technology), la FIDO Alliance a publié en juin 2023 le livre blanc FIDO Authentication for Moderate Assurance Use Cases.

Ce document fournit des recommandations pour l'analyse des capacités et des fonctionnalités des passkeys liées à un terminal et des passkeys synchronisées, afin de pouvoir déterminer comment ces deux types d'identifiants peuvent être utilisés dans un environnement à niveau d'assurance modéré. (Ce dernier est défini comme présentant plusieurs cas d'usage d'authentification différents qui peuvent être résolus par une combinaison de niveaux d'assurance 1 et/ou 2 et 3.)

Remarque : le NIST travaille actuellement à mettre à jour les niveaux d'assurance dans le contexte des passkeys synchronisées. Assurez-vous donc de consulter les dernières ressources du NIST et de la FIDO Alliance pour obtenir les informations les plus récentes.

Les passkeys sont plus pratiques que les mots de passe

En remplaçant les processus d'authentification fastidieux par un balayage avec le doigt, la reconnaissance faciale, la saisie d'un code PIN ou une autre action de déverrouillage courante, les passkeys synchronisées réduisent considérablement les frictions rencontrées par les utilisateurs lorsqu'ils interagissent avec des services en ligne.

Il est d'ailleurs révélateur que certaines des premières entreprises à avoir adopté les passkeys, notamment Shopify, DocuSign et PayPal, offrent des expériences utilisateurs sécurisées et *pratiques*.

Pour de nombreux fournisseurs de services, la plus grande facilité d'emploi des passkeys synchronisées pourrait même être leur principal avantage. Alors que les passkeys liées à un terminal exigent des utilisateurs qu'ils s'inscrivent sur chaque site web ou dans chaque application sur chaque terminal, les passkeys synchronisées :

- permettent aux utilisateurs d'accéder automatiquement à leurs identifiants de connexion FIDO sur plusieurs terminaux (même nouveaux) ;
- permettent aux utilisateurs de récupérer leurs passkeys même s'ils perdent tous leurs terminaux.

Dans le cas des entreprises commerciales, les frictions (c'est-à-dire tout ce qui ralentit les interactions d'une personne avec un service) constituent un obstacle important aux conversions et, par extension, à l'augmentation de leurs recettes. D'après le rapport Okta Customer Identity Trends Report, près de 60 % des personnes interrogées se disent plus susceptibles de dépenser de l'argent lorsque les services proposent un processus de connexion simple, fluide et sécurisé. Cette constatation s'applique à tous les secteurs d'activité, ce qui suggère que les utilisateurs recherchent la praticité dans toutes leurs interactions.

Bien qu'il existe des différences entre les régions, ce sont les tranches d'âge qui présentent la variation la plus importante : les plus jeunes sont environ un tiers plus susceptibles que les plus âgés de dépenser davantage d'argent pour une expérience de connexion simple, fluide et sécurisée (figure 1).

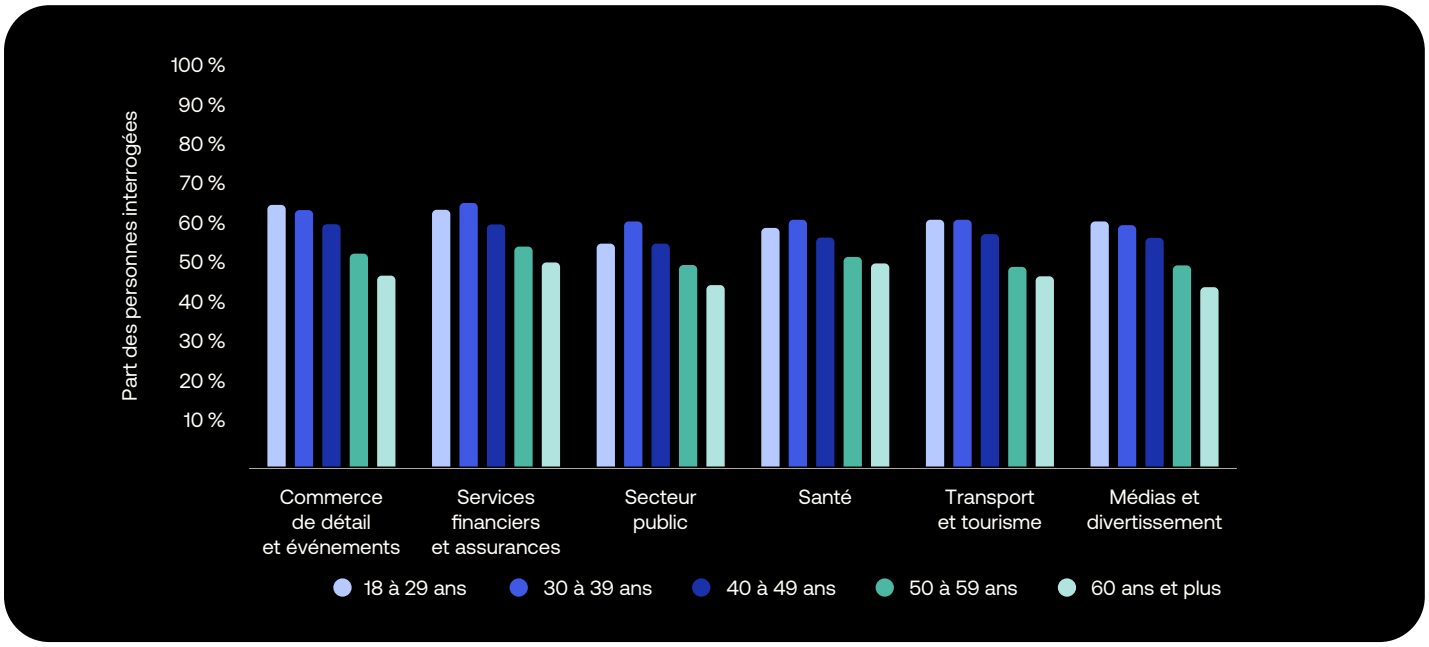


Figure 1. Lorsque vous interagissez avec une marque en ligne, diriez-vous que vous êtes plus ou moins susceptible de dépenser de l'argent si vous savez que le processus de connexion est simple, fluide et sécurisé ? Les graphiques montrent la somme des réponses « Très susceptible » et « Relativement susceptible ».

Bien entendu, un certain degré de friction est nécessaire pour établir la confiance et mettre en œuvre des contrôles de sécurité, mais la réduction des frictions chaque fois que possible, dans toutes les interactions des consommateurs, peut accroître les taux de conversion et, par conséquent, augmenter les revenus à court et long terme.

Examinons maintenant quelques façons dont les passkeys génèrent moins de frictions que les mots de passe.

Les passkeys synchronisées sont plus rapides à utiliser que les mots de passe

Des études montrent qu'outre leur facilité d'utilisation, les passkeys synchronisées sont également bien plus rapides que les mots de passe. Dans un article publié sur son blog dédié à la sécurité, Google explique qu'il faut en moyenne 14,9 secondes pour se connecter avec une passkey, soit près de deux fois moins que les 30 secondes nécessaires avec un mot de passe.

L'article précise que les données préliminaires et qualitatives issues des études axées sur les utilisateurs indiquent également que les utilisateurs perçoivent déjà cette praticité comme le principal avantage des passkeys.

Les passkeys sont plus accessibles que les mots de passe

Si les points de friction incommodent de nombreux consommateurs, ils peuvent empêcher certains utilisateurs d'accéder à vos services.

Mettez-vous à la place d'un utilisateur avec une déficience visuelle, un trouble cognitif ou des fonctions motrices limitées devant se soumettre à un flux d'authentification fastidieux qui exige de mémoriser et de saisir un mot de passe long et complexe, même par « simple » copier-coller. Imaginez la réaction d'un utilisateur peu averti ou technophobe lorsqu'un message va lui demander de télécharger une application d'authentification.

Les passkeys offrent une alternative bien plus accessible à d'autres approches traditionnelles.

Être attentif à l'accessibilité tout au long du parcours client offre également des résultats sur le plan financier. En créant des expériences accessibles à tous, les marques peuvent étendre la portée de leur offre sur le marché.

Les passkeys synchronisées rendent l'authentification forte plus pratique

Les passkeys synchronisées rendent même la sécurité renforcée plus pratique, car elles vérifient l'identité et la clé privée d'un utilisateur en une seule étape (du point de vue de l'utilisateur) — une nette amélioration par rapport aux autres techniques MFA.

Cette facilité d'emploi accrue permet également aux fournisseurs de services d'envisager une réauthentification à une fréquence plus élevée ou en tant qu'authentification renforcée (p. ex. pour accéder aux applications sensibles, apporter des modifications à un compte, accéder à des données privées, etc.). Ces deux mesures constituent des défenses critiques contre le piratage de session. Comme mentionné dans le rapport **Okta Secure Sign-in Trends Report 2023**, la résolution des demandes d'authentification utilisant WebAuthn nécessite en moyenne trois secondes seulement. Elle est donc nettement plus rapide que la combinaison des mots de passe et des demandes d'authentification OTP.

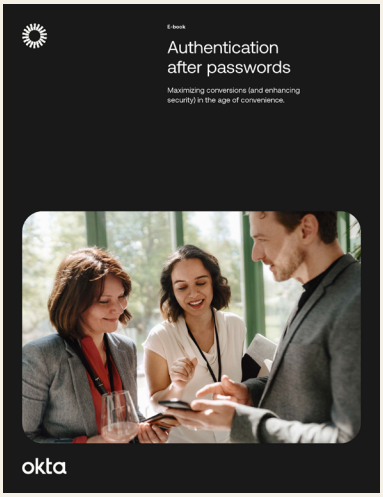
Les passkeys synchronisées sont plus faciles à créer que les mots de passe

Naturellement, les utilisateurs ne peuvent profiter de ces avantages qu'après avoir créé une passkey synchronisée. Le processus doit donc être simple. Les inscriptions répétées requises par les passkeys liées à un terminal sont souvent citées comme l'une des principales raisons pour lesquelles l'adoption de WebAuthn est aussi limitée, en particulier auprès du grand public.

En permettant aux identifiants FIDO d'un utilisateur de transiter facilement (mais de manière sécurisée) sur une multitude de terminaux, les passkeys synchronisées résolvent ce problème : l'inscription elle-même est simple et n'intervient qu'une fois par service.

De fait, l'enquête Okta « Secure Sign-In Trends Report » révèle que la durée médiane de création d'un mot de passe avoisine les 34 secondes, ce qui inclut le temps nécessaire pour créer un nouveau mot de passe et le confirmer (c'est-à-dire le saisir à nouveau). L'inscription basée sur WebAuthn prend seulement 19 secondes, ce qui remet en cause l'idée selon laquelle les authentificateurs à niveau d'assurance plus élevé constituent un point de friction important pour les utilisateurs lors de l'inscription.

Il est probable que si, au départ, de nombreux utilisateurs ne seront pas familiarisés avec les passkeys synchronisées, ils trouveront rapidement l'inscription au moins aussi intuitive que les autres mécanismes d'authentification, et bien plus rapide.



Les passkeys synchronisées représentent une étape importante vers un monde sans mot de passe

En offrant une sécurité des comptes renforcée par rapport aux mots de passe et des expériences utilisateurs plus pratiques, les passkeys synchronisées ont de bonnes chances de populariser l'authentification sans mot de passe bien au-delà des administrateurs IT (qui priorisent la sécurité) et des premiers adeptes (qui ont conscience des nombreux avantages).

Téléchargez notre guide complet, **Authentication After Passwords** pour en savoir plus sur l'avenir sans mot de passe, y compris les idées fausses les plus répandues (sur les flux sans mot de passe déjà présents à votre insu, par exemple) et les mesures à prendre pour conserver une longueur d'avance sur la concurrence.

Pour en savoir plus sur la propre transition d'Okta vers un modèle sans mot de passe, consultez l'article **Why we're going 100% passwordless at Okta**.

Fonctionnement des passkeys

Comme l'explique la FIDO Alliance, les protocoles FIDO sous-jacents emploient des techniques de cryptographie à clé publique standard pour appliquer une authentification forte. Pour s'inscrire à un service en ligne, le terminal de l'utilisateur crée une nouvelle paire de clés cryptographiques constituée des éléments suivants :

- Une clé publique, qui est enregistrée auprès du service en ligne
- Une clé privée, qui est conservée comme un véritable secret

Les clés sont générées de manière sécurisée et unique pour chaque compte. Vous n'avez donc pas à craindre que des utilisateurs choisissent une clé privée faible, et les clés privées ne sont pas réutilisées pour plusieurs services.

Pour s'authentifier auprès d'un service particulier, le terminal client prouve la possession de la clé privée correspondante du compte en signant une demande d'authentification fournie par le service. Le service lui-même ne voit jamais la clé privée et, par extension, n'a jamais besoin de la stocker ni de la protéger.

Il est important de noter que la clé privée ne peut être utilisée qu'après avoir été déverrouillée par l'utilisateur. Le déverrouillage local passe souvent par l'insertion d'un terminal faisant office de deuxième facteur ou via le mécanisme de déverrouillage du terminal principal, en général un code PIN ou une authentification biométrique (Touch ID, Face ID, Windows Hello, etc.).

Voici en quoi les passkeys synchronisées diffèrent des implémentations FIDO2 antérieures :

- Elles peuvent être utilisées sur n'importe quel terminal dans un écosystème particulier où les passkeys sont sauvegardées sur le terminal et dans le cloud.
- Les utilisateurs peuvent effectuer une authentification multi-terminaux pour franchir facilement les frontières de l'écosystème sans être confrontés aux frictions associées à la création d'identifiants FIDO sur de nouveaux terminaux.

Pour en savoir plus sur les mécanismes sous-jacents du fonctionnement des passkeys, consultez le site web de la FIDO Alliance.

Implémentation des passkeys dans une application

Généralement, les développeurs suivent deux approches pour étendre l'authentification en vue de prendre en charge les passkeys :

- Ils implémentent les passkeys eux-mêmes via des API et des SDK.
- Ils font appel à un fournisseur de services d'identité.

Plus d'informations sur le déploiement des passkeys

La FIDO Alliance a publié une série de livres blancs destinés aux administrateurs IT, aux architectes de sécurité d'entreprise et aux cadres dirigeants qui envisagent de déployer l'authentification FIDO dans leur entreprise.

L'approche « maison »

Du point de vue de l'implémentation, les passkeys synchronisées ressemblent beaucoup à des authentificateurs de plateforme ne fournissant pas de déclaration d'attestation. Du point de vue du protocole, si votre application web prend déjà en charge WebAuthn, tant qu'elle ne requiert pas de réponse d'attestation, vous prenez techniquement déjà en charge les passkeys synchronisées. Du point de vue de l'expérience utilisateur, par contre, ce n'est pas forcément le cas. Par exemple :

- Les invites et le langage utilisés sur vos pages d'inscription actuelles font probablement référence à des identifiants liés à un terminal (p. ex. « Connectez-vous plus rapidement sur ce terminal »), ce qui n'est plus totalement vrai avec les passkeys synchronisées.
- Il y a de fortes chances que vous utilisiez des authentificateurs de plateforme pour prendre en charge uniquement des facteurs d'authentification secondaires, étant donné qu'avant le déploiement des passkeys synchronisées, vous étiez directement responsable de la récupération de comptes.

Aucun des changements ci-dessus n'est particulièrement difficile à mettre en place, surtout si vous avez déjà implémenté WebAuthn, mais vous avez un peu de travail pour proposer une expérience de qualité.

Pour aider les développeurs, en octobre 2022, le W3C WebAuthn Community Adoption Group et la FIDO Alliance ont lancé passkeys.dev, une ressource en ligne contenant de la documentation et suivant la prise en charge des terminaux, entre autres.

Identity Unlocked

Focus sur les passkeys avec Andrew Shikiar et Tim Cappalli

Peu de temps après l'annonce des passkeys synchronisées (en tant qu'identifiants multi-terminaux), Andrew Shikiar (Executive Director et CMO de la FIDO Alliance) et Tim Cappalli (Digital Identity Standards Architect chez Microsoft) ont rencontré Vittorio Bertocci (Principal Architect chez Auth0), présentateur du **podcast Identity Unlocked**.

Écoutez l'épisode pour en savoir plus sur l'évolution des identifiants FIDO et obtenir des informations destinées aux développeurs sur le fonctionnement des identifiants multi-terminaux.

Le recours à un fournisseur de services d'identité

La gestion des identités est une tâche complexe, et la mise en place d'implémentations efficaces reste un processus difficile même pour les professionnels les plus aguerris. Qui plus est, les attentes des clients sont de plus en plus élevées. Les utilisateurs comparent chaque expérience aux meilleures qu'ils ont rencontrées, ce qui place une pression importante sur les entreprises appelées à sans cesse améliorer leur expérience utilisateur.

Toutefois, les besoins en matière d'identité doivent être satisfaits en ménageant les précieuses ressources d'ingénierie nécessaires pour renforcer les compétences clés, et ces deux objectifs doivent être atteints sans négliger les exigences réglementaires ni compromettre la sécurité.

Pour ces raisons, de nombreuses entreprises jugent plus efficace et rentable d'intégrer un service d'identité à leurs applications et à leur pile technologique. Par ailleurs, un partenariat avec un fournisseur de services d'identité aide les entreprises à répondre à un plus vaste ensemble d'exigences en matière de gestion des identités et des accès clients (CIAM), dont les suivantes :

- Authentification
- Autorisation
- Gestion des utilisateurs

Il est certain que les fournisseurs d'identité établis prendront en charge les passkeys, afin d'offrir une alternative pratique aux développeurs d'applications souhaitant élargir leurs options d'authentification et suivre l'évolution rapide du paysage de l'authentification.

Par exemple, si vous possédez déjà une application configurée pour utiliser Okta Customer Identity Cloud pour l'authentification, vous pourrez activer les passkeys sans même toucher à votre code.

Toutefois, les fournisseurs d'identité ne proposent pas tous les mêmes caractéristiques et fonctionnalités. Nous vous recommandons donc vivement de faire preuve de vigilance. Voici néanmoins quelques caractéristiques ou fonctionnalités à prendre en compte dans votre décision :

- Indépendance et neutralité → Votre solution CIAM doit multiplier vos possibilités d'action, pas les limiter. Autrement dit, elle doit pouvoir s'intégrer à vos solutions existantes, s'appuyer sur des normes ouvertes afin d'éviter tout effet de captivité ou encore être compatible avec votre fournisseur de services cloud.
- Fonctions complètes et personnalisables → Chaque client est unique et ses besoins sont complexes. Votre solution CIAM doit vous aider à créer des expériences fluides, cohérentes et fiables, et ce, pour chaque type d'utilisateur.
- Facilité d'exploitation, de maintenance et d'utilisation → Quasiment à chaque fois qu'elles intègrent une nouvelle technologie, les équipes d'ingénierie cherchent à réduire les efforts et les coûts liés à son déploiement, à sa configuration et à son exécution, et votre solution CIAM doit respecter ce principe.
- Fiabilité → En cas de brèche de sécurité importante, de non-respect des exigences de conformité ou d'indisponibilité ou dégradation des services, les conséquences juridiques, financières ou pour votre réputation peuvent être considérables. Votre solution CIAM doit pouvoir vous apporter une certaine sérénité face à ces risques.

Et ensuite ?

Lorsque WebAuthn a vu le jour, Auth0 (désormais Okta Customer Identity Cloud) a immédiatement perçu sa valeur ajoutée et l'a adopté comme deuxième facteur pour les administrateurs accédant à notre tableau de bord de gestion et comme méthode que les développeurs peuvent utiliser pour authentifier leurs utilisateurs lorsqu'ils protègent leurs applications web.

Cependant, malgré ses avantages évidents en termes de sécurité, l'adoption de l'authentification FIDO2 dans les applications grand public est restée jusqu'à présent assez faible. Nos propres observations indiquent qu'elle semble être principalement utilisée par des professionnels qui ont besoin d'un niveau d'assurance élevé lorsqu'ils accèdent aux ressources qu'ils gèrent.

Il y a beaucoup d'explications possibles, mais voici le consensus qui se dégage :

- Les clés physiques sont principalement réservées aux administrateurs et aux principaux professionnels de la connaissance, plutôt qu'au marché grand public plus large.
- Bien que les authentificateurs de plateforme soient plus satisfaisants, le fait qu'ils soient liés à un seul terminal (une fonctionnalité potentiellement convoitée dans les scénarios d'entreprise) présente des problèmes de facilité d'utilisation pour le grand public, car les utilisateurs possèdent souvent de nombreux terminaux et en acquièrent régulièrement de nouveaux.

Mais l'avènement des passkeys synchronisées — et l'influence considérable d'Apple, de Google, de Microsoft et d'autres entreprises de premier plan — pourrait représenter un important point d'inflexion. Certains utilisateurs les plébisciteront, d'autres se montreront plus hésitants, mais dans les mois et années à venir, les passkeys deviendront omniprésentes.

De façon plus générale, l'authentification sans mot de passe deviendra plus courante. Son adoption sera stimulée par des expériences utilisateurs positives et des avantages en termes de sécurité. Les entreprises qui mettent les passkeys et d'autres mécanismes d'authentification sans mot de passe à disposition des clients et d'autres utilisateurs en tireront profit.

Il faut reconnaître que certains problèmes restent sans réponse. Par exemple :

- Les passkeys sont résistantes au phishing, mais l'onboarding d'un nouvel utilisateur avec une passkey et un moyen de récupération (p. ex. le compte de messagerie associé à l'écosystème du système d'exploitation) représente une vulnérabilité potentielle.
- Pour le moment, l'expérience utilisateur varie selon les écosystèmes et les gestionnaires de mots de passe. La FIDO Alliance s'efforce d'améliorer la cohérence mais, du moins à court terme, les expériences incohérentes restent d'actualité et peuvent être source de frustration pour certains utilisateurs.
- Comme nous l'avons mentionné précédemment, nous ne savons pas encore où se situent les passkeys synchronisées dans le framework de niveaux d'assurance du NIST. Cette question est importante dans un monde où de nombreux collaborateurs utilisent leur terminal personnel pour accéder à des ressources d'entreprise protégées.
- Enfin, comme toute introduction de nouvelle technologie, la sensibilisation du grand public aux passkeys demeure un défi permanent, notamment en ce qui concerne la sécurité, la confidentialité et la praticité.

Il convient de rappeler que les passkeys sont très récentes et que la situation globale continuera d'évoluer à mesure que des implémentations apparaissent et sont optimisées.

Le mieux est l'ennemi du bien

On peut raisonnablement affirmer que les problèmes associés aux passkeys sont éclipsés par les problèmes liés aux mots de passe. Les mots de passe doivent disparaître, ou du moins devenir beaucoup moins répandus, et tous les acteurs du secteur de l'identité doivent chercher des moyens de tirer parti des avantages des passkeys tout en limitant leurs inconvénients.

Chez Okta, nous tenons à faire notre part en proposant des fonctionnalités de pointe, opportunes et orientées développeurs prenant en charge les passkeys, ainsi qu'en participant activement aux discussions sectorielles qui façonnent l'avenir de cette technologie.

Il deviendra plus facile d'adopter l'authentification sans mot de passe à mesure que les fournisseurs de plateforme et les fabricants de terminaux s'aligneront sur des flux normalisés pour la récupération, l'émission et la non-prolifération. Nous recommandons à ceux qui souhaitent déployer ou étendre l'authentification sans mot de passe de rechercher des authentificateurs offrant les avantages suivants :

- Authentification sans points de friction
- Réduction des erreurs de connexion
- Inscription simple des utilisateurs
- Résistance aux tentatives de phishing

Pour information, les passkeys répondent à tous ces critères.