okta

Principe de fonctionnement de WebAuthn

Okta France
Paris

paris@okta.com
01 85 64 08 80

WebAuthn

Ces dernières années, le nombre de sites web dont les données clients sont tombées entre de mauvaises mains a grimpé en flèche. Les pertes dues aux fraudes et au piratage de comptes se chiffrent à plus de 5,1 milliards de dollars, et de grandes sociétés orientées client, comme Marriott Starwood et Google, ont été victimes de brèches de sécurité à grande échelle. Face à la perte de confiance des consommateurs et à un manque à gagner de plusieurs millions, les entreprises doivent revoir leur approche de la protection des utilisateurs.

1re partie : WebAuthn et ses conséquences économiques

En mars 2019, le World Wide Web Consortium (W3C) annonçait que WebAuthn était désormais le standard web officiel pour les connexions sans mot de passe. WebAuthn, pris en charge par un grand nombre d'applications, devrait connaître une adoption massive dans les années à venir.

Avec cette nouvelle norme, n'importe quelle application web exécutée dans un navigateur compatible peut désormais tirer parti des terminaux enregistrés comme authentificateurs pour identifier les utilisateurs de manière sécurisée. La prise en charge par Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari et Opera, sans oublier l'adoption rapide par différentes plateformes (Microsoft Edge avec Windows Hello, Google Android, etc.), signifie qu'il existe enfin un moyen pratique de déployer FIDO2/WebAuthn. Par le passé, l'absence de navigateurs et de plateformes compatibles avait considérablement freiné l'adoption de la norme U2F. Aujourd'hui, les entreprises peuvent utiliser des jetons externes (des clés YubiKey, par exemple) ou se servir directement des plateformes prises en charge, puisque le terminal lui-même est utilisé pour WebAuthn.

Avantages pour l'équipe IT et le consommateur

WebAuthn a de nombreuses retombées positives sur les utilisateurs comme sur les entreprises. Non seulement il permet d'améliorer l'expérience utilisateur (grâce à la connexion sans mot de passe, par exemple), mais il offre en outre une sécurité renforcée aux entreprises comme aux consommateurs, et limite les attaques dont ils pourraient faire l'objet.

En utilisant WebAuthn, les entreprises protègent leurs sites web des attaques multisites automatisées basées sur l'usage en masse de mots de passe piratés (password spraying/stuffing, par exemple). Cette norme offre également des avantages pour les utilisateurs, dont les identifiants de connexion sont la cible privilégiée de ces attaques. Nous verrons en deuxième partie quels sont les premiers bénéficiaires de WebAuthn.

Pour les clients et les utilisateurs finaux, le principal avantage est la prévention du piratage de comptes découlant d'un vol d'identifiants par phishing. Dans la mesure où WebAuthn enregistre l'authentificateur auprès d'une application spécifique, crée une paire de clés publique/privée et stocke les informations d'identification en local dans des authentificateurs intégrés (Microsoft Edge, Android, etc.) ou externes (clés YubiKey, etc.), ces identifiants sont difficiles à subtiliser par phishing.

WebAuthn permet aux utilisateurs de prendre en main leur sécurité plutôt que de se reposer entièrement sur une entité spécialisée pour stocker correctement leurs identifiants, en espérant qu'ils ne seront pas piratés. En outre, WebAuthn étant désormais relativement simple d'emploi, il y a fort à parier que cette méthode d'authentification forte saura s'imposer auprès d'autres types d'utilisateurs.

2e partie : Histoire de l’authentification

Points faibles des méthodes d’authentification actuelles

Avant de chercher à savoir pourquoi WebAuthn a été créé et de s’intéresser à ses diverses fonctionnalités, il est important de revenir sur les débuts de l’authentification utilisateur et de cerner les points faibles des méthodes actuelles.

Authentification par mot de passe

Nous sommes tous habitués à nous authentifier à l’aide de noms d’utilisateur et de mots de passe. Bien que cette méthode soit omniprésente et à la portée de tous, un Américain sur cinq a déjà été victime d’un piratage de compte à la suite d’un vol de mot de passe. Sachant qu’un utilisateur possède en moyenne plus de 130 comptes en ligne, les entreprises ont tout intérêt à faire évoluer leur framework d’authentification pour préserver leur activité.

Authentification à deux facteurs

La nouvelle méthode d’authentification la plus fréquente est l’authentification à deux facteurs (2FA). Mais dans le cas des comptes clients, les facteurs secondaires courants tels que les SMS sont bien connus pour leur vulnérabilité aux attaques par phishing. Face au manque de fiabilité de l’authentification 2FA, WebAuthn constitue une solution potentielle pour contrer le phishing et améliorer l’expérience client.

Qu’est-ce que WebAuthn ?

Nouveau standard mondial d’authentification web, WebAuthn est une API pour navigateurs qui simplifie et sécurise l’accès aux applications web en utilisant des terminaux enregistrés (téléphones, ordinateurs portables, etc.) comme facteurs d’authentification. Elle fait appel à la cryptographie à clé publique pour protéger les utilisateurs des attaques sophistiquées par phishing.

Avantages de WebAuthn et parties prenantes

WebAuthn présente trois grands avantages pour les parties prenantes, notamment les clients, les responsables produits, les équipes de sécurité et les services d'assistance.

Avantages	Parties prenantes
Amélioration de l'engagement client	Clients, responsables produits
Renforcement de la sécurité	Clients, équipes de sécurité
Réduction de la charge de travail du service d'assistance • **Utilisation de WebAuthn comme méthode de connexion principale** • **Rétrocompatibilité**	Assistance

Amélioration de l'engagement client

Clients - Offrir une expérience de connexion fluide

Puisque WebAuthn utilise le terminal comme facteur d'authentification, plus aucun mot de passe n'est nécessaire. Côté client, il n'est plus nécessaire de mémoriser des noms d'utilisateur et mots de passe pour la connexion, ou de demander un mot de passe à usage unique dans le cas d'une authentification à deux facteurs. Le processus est donc simplifié pour l'utilisateur final, qui doit simplement se servir de son terminal enregistré pour s'authentifier.

Responsables produits - Écourter les délais d'authentification

Comme nous le disions, WebAuthn élimine la nécessite de recourir aux mots de passe. Soucieux que leurs applications rencontrent un large public, les responsables produits s'emploient généralement à supprimer tous les obstacles qui se dressent sur le parcours de leurs clients. Grâce à WebAuthn, ils ont la possibilité d'offrir une expérience de connexion fluide à ces utilisateurs.

Responsables produits - Écourter les délais de lancement

De plus, libérés du casse-tête des mots de passe, ces responsables produits peuvent accélérer le lancement de leurs produits sans avoir à déployer des architectures complexes pour gérer et stocker les mots de passe.

Renforcement de la sécurité

Clients - Préserver la confiance

Face à la multiplication des brèches de sécurité, il est particulièrement important de préserver la confiance des clients. Ces derniers vous confient leurs informations et veulent l'assurance que les données qu'ils partagent sont protégées. Avec WebAuthn, vous bénéficiez d'une méthode d'authentification beaucoup plus sûre, qui écarte les risques associés aux mots de passe.

Équipes de sécurité - Éliminer les faiblesses inhérentes aux mots de passe

Contrairement aux autres méthodes d'authentification, WebAuthn ne repose pas sur des facteurs de connaissance, tels que les noms d'utilisateur et les mots de passe, mais sur les terminaux enregistrés qui appartiennent à l'utilisateur final. Ces appareils étant plus difficiles à dérober que les mots de passe, le risque d'usurpation d'identité est plus faible, à la grande satisfaction des équipes de sécurité.

Réduction de la charge de travail du service d'assistance

Service d'assistance - Réduire les cycles de support indissociables de l'authentification multifacteur

La norme WebAuthn a la particularité de pouvoir être utilisée comme méthode de connexion principale. Son implémentation simplifie les cycles de support, car le nombre de facteurs se limite tout simplement à WebAuthn.

Service d'assistance - Tirer parti de la rétrocompatibilité

WebAuthn offre des caractéristiques de rétrocompatibilité, ce qui évite aux entreprises d'actualiser immédiatement les jetons déjà distribués. Les clés FIDO U2F, notamment les clés YubiKey de type U2F, restent ainsi utilisables comme facteurs secondaires dans les navigateurs web compatibles avec WebAuthn, ce qui laisse davantage de temps aux entreprises pour opérer ou planifier leur migration.

3e partie : Principe de fonctionnement de WebAuthn (utilisations et interface d'Okta)

Après avoir évoqué quelques-uns des avantages offerts par WebAuthn en termes d'expérience client et de renforcement de la sécurité, nous allons à présent aborder les différentes utilisations de cette norme et les bonnes pratiques correspondant à chaque étape du processus WebAuthn.

Principales utilisations de WebAuthn

Processus d'inscription

Processus d'authentification

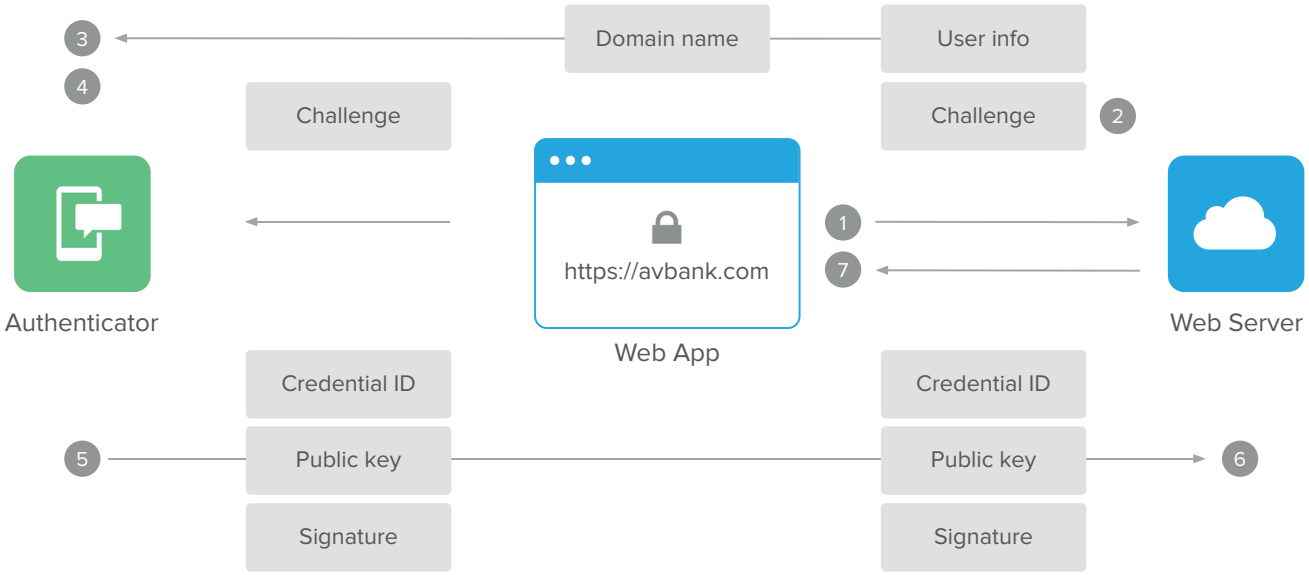
Récupération de comptes

Processus d'inscription

L'inscription est le processus au cours duquel l'utilisateur lie son authentificateur (terminal) au serveur web. Ce processus fait appel à trois éléments principaux : l'authentificateur, l'application web et le serveur web. En voici les différentes étapes :

Informations d'identification	q2we323d2rty123
Clé privée	s12ds3d4s5da6
Nom de domaine	avbank.com
Informations utilisateur	Swaroop Sham

Utilisateur	Jason Sham
Clé de challenge	a9ds9dw9eds9d
Informations d'identification	q2we323d2rty123
Clé publique	0x3idfkek309



1. L'utilisateur lance la configuration de son terminal.
2. Le serveur web génère une clé de challenge (à usage unique) pour l'enregistrement.
3. Le serveur web envoie la clé de challenge et les informations utilisateur à l'application web.
4. L'application web ajoute le nom du domaine faisant autorité aux informations à transmettre à l'authentificateur.
5. L'authentificateur demande le consentement de l'utilisateur.
6. Une fois ce consentement obtenu, l'authentificateur enregistre l'identifiant, les clés publique et privée, les informations utilisateur et le nom du domaine.
7. L'application web transmet l'identifiant, la clé publique et la signature au serveur web.
8. La clé de challenge est invalidée et le terminal est enregistré.

Cas d'usage 1 - Inscription avec Okta

Avec Okta, les utilisateurs peuvent enregistrer un authentificateur « plateforme » lors du processus d'identification du tenant de votre entreprise. En définissant des options de connexion et des politiques d'inscription à l'authentification multifacteur, les administrateurs peuvent activer l'authentification web des utilisateurs via l'indicateur de fonctionnalité. De son côté, l'utilisateur final, une fois qu'il a saisi son nom d'utilisateur et son mot de passe, a la possibilité de s'inscrire à Windows Hello, l'authentificateur "plateforme" de Windows (figure 1). Il s'agit de la première étape du processus d'inscription.

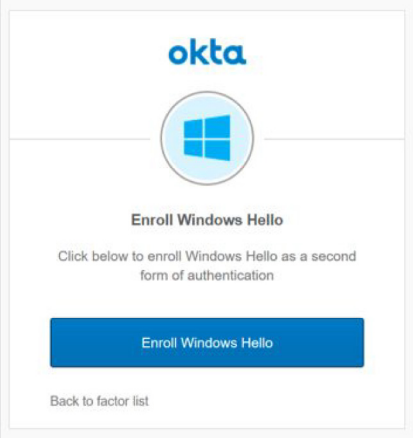


Figure 1

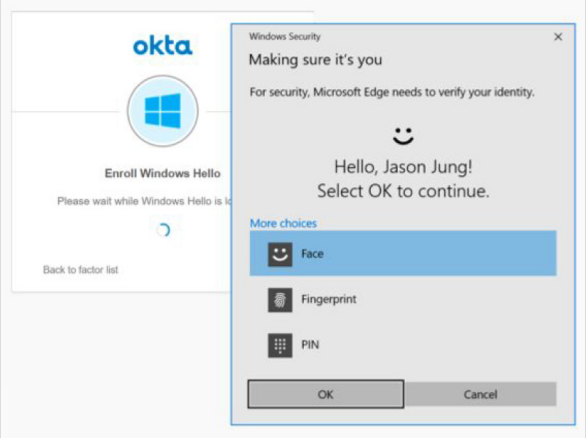
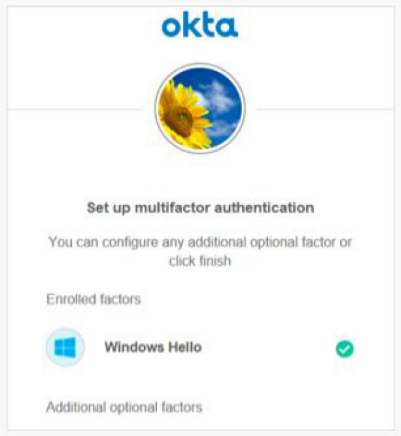


Figure 2

En supposant que Windows Hello ait été configuré, un paramétrage à usage unique permettrait de créer une paire de clés publique/privée (étape 5). Comme pour le processus d'inscription illustré ci-dessus, l'utilisateur donnerait son consentement par reconnaissance faciale ou empreintes digitales, ou en saisissant le code PIN stocké sur son terminal.

Une fois le consentement accordé (sous forme de facteur biométrique ou de code PIN), l'identifiant, la clé publique et la signature seraient envoyés au serveur web chargé de l'inscription.



Bonnes pratiques d'Okta

Pour réduire les risques inhérents à cette étape, il est conseillé de restreindre l'inscription, dans un premier temps, à la période pendant laquelle les utilisateurs se trouvent dans le périmètre du réseau de l'entreprise et de limiter les fenêtres d'inscription (par exemple en obligeant les nouveaux utilisateurs à s'inscrire dans les trois jours qui suivent leur arrivée).

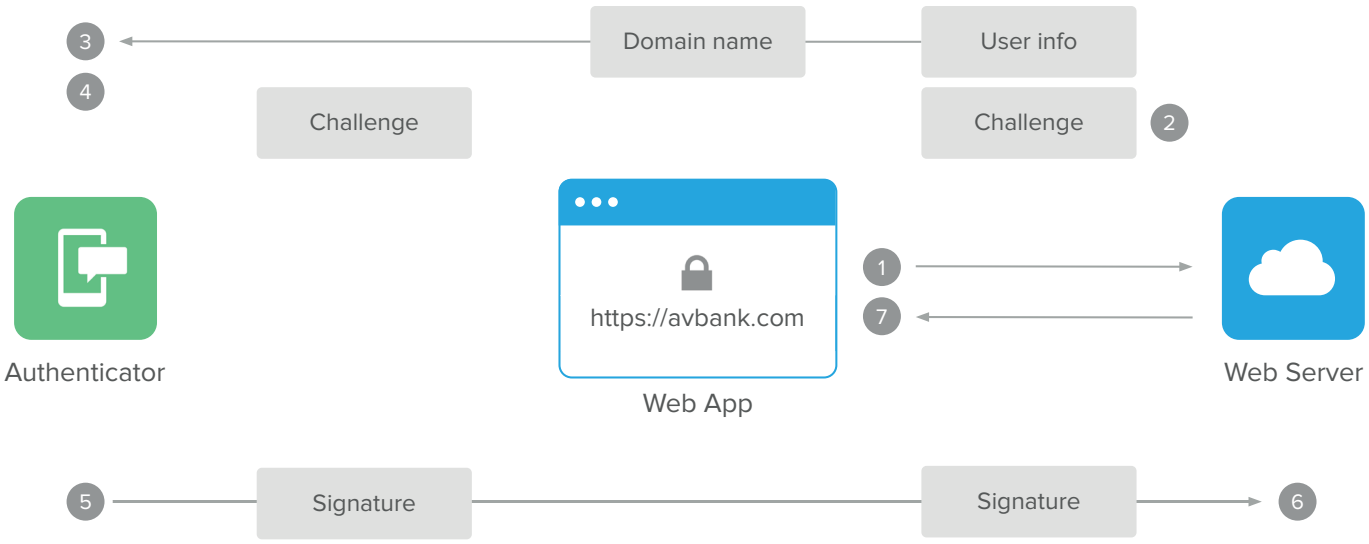
Dans la liste des bonnes pratiques, citons également des fonctionnalités telles que la visibilité de l'utilisateur final sur l'inscription et la récupération des facteurs d'authentification ; les politiques d'inscription propres à une application (par exemple restrictions d'accès associées à certaines applications) ; ou encore la mise en place de processus personnalisés pour la vérification des identités lors de l'inscription.

Principe de fonctionnement de l'authentification

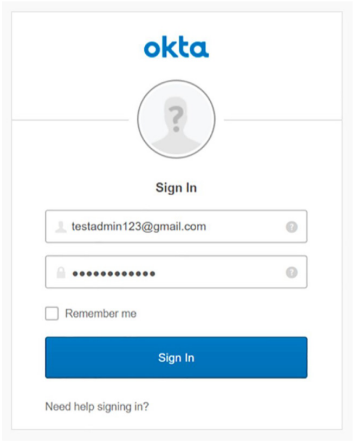
Une fois le terminal inscrit, l'authentification des utilisateurs avec WebAuthn est fluide et sécurisée. L'inscription ayant déjà eu lieu, ce flux d'authentification consiste pour l'essentiel à générer une signature à partir de la clé privée stockée sur l'authentificateur, ce qui aboutit à chaque fois à la création d'une demande d'authentification (challenge).

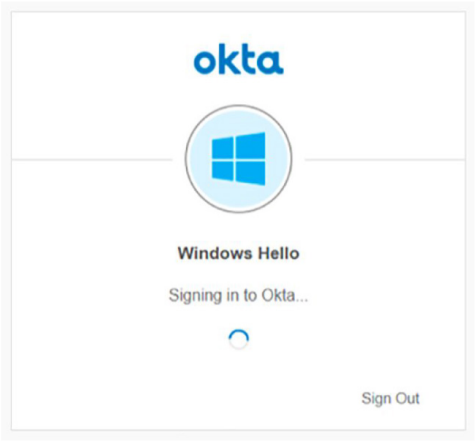
Informations d'identification	q2we323d2rty123
Clé privée	s12ds3d4s5da6
Nom de domaine	avbank.com
Informations utilisateur	Swaroop Sham

Utilisateur	Jason Sham
Clé de challenge	a9ds9dw9eds9d
Informations d'identification	q2we323d2rty123
Clé publique	0x3idfkek309



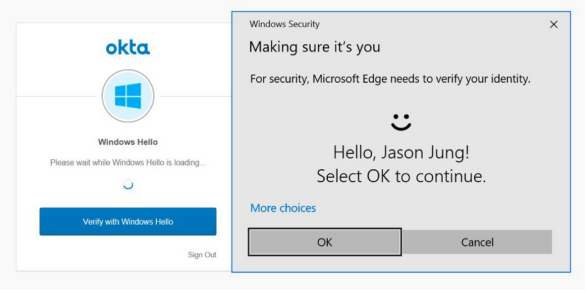
1. L’utilisateur lance la configuration de son terminal.
2. Le serveur web crée une demande d’authentification (challenge) unique et le transmet à l’authentificateur.
3. L’authentificateur reçoit la demande d’authentification avec le nom de domaine correspondant.
4. L’authentificateur reçoit le consentement biométrique de l’utilisateur.
5. L’authentificateur génère une signature cryptographique et l’envoie au serveur web.
6. Le serveur web vérifie la signature en déchiffrant la demande d’authentification unique pour connecter l’utilisateur.
7. L’utilisateur est connecté.





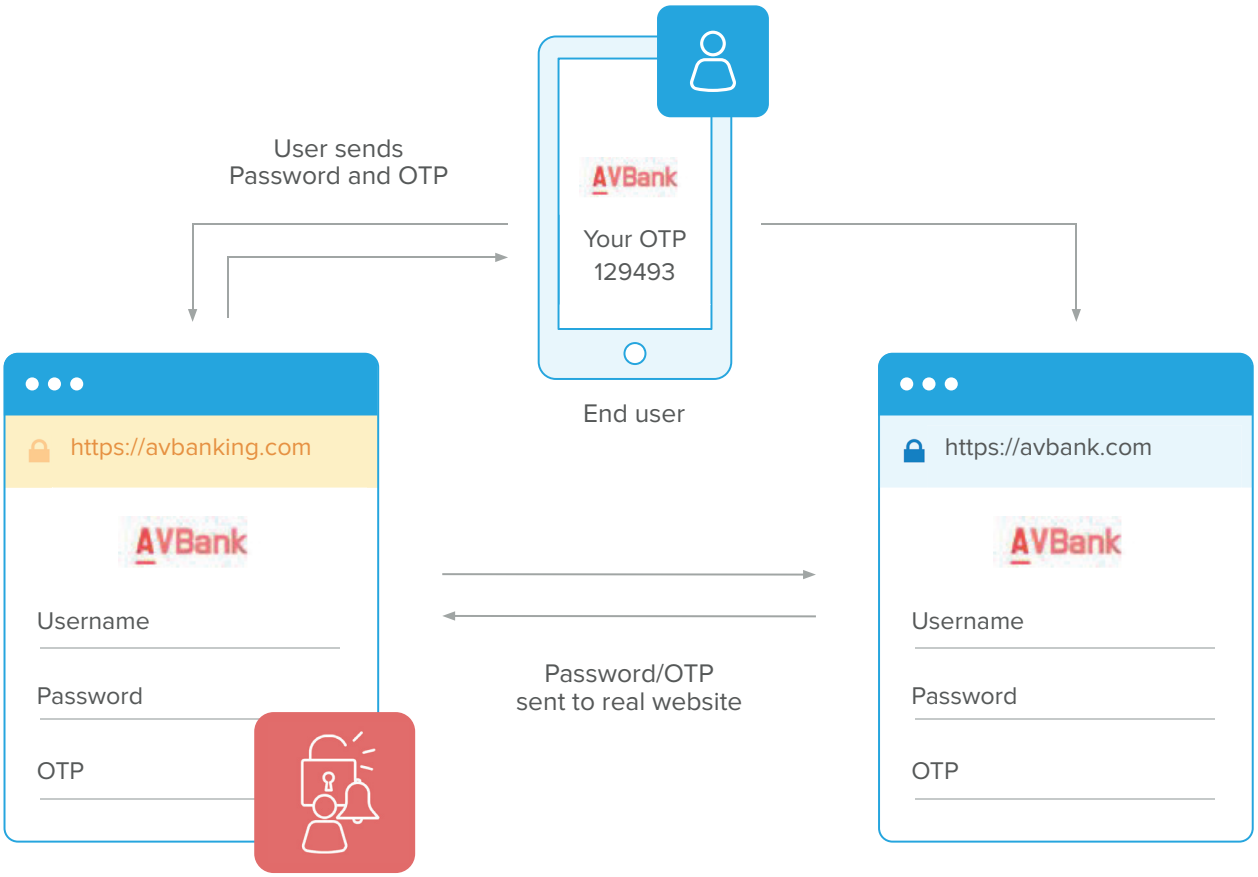
Cas d’usage 2 - Authentification avec Okta

Avec Okta, les utilisateurs peuvent se servir d’authentificateurs de plateformes qui remplacent l’authentification renforcée. Après avoir saisi leurs nom d’utilisateur et mot de passe, ils peuvent utiliser WebAuthn comme facteur de sécurité supplémentaire. Okta peut également être configuré pour créer une demande d’authentification (challenge) en fonction notamment de la zone réseau, de l’heure ou du type de terminal. Pour s’authentifier dans Okta, l’utilisateur serait invité à s’identifier dans Windows Hello.



WebAuthn et le phishing

La résistance de WebAuthn aux attaques par phishing s'explique par l'enregistrement du nom de domaine sur l'authentificateur. La plupart des attaques de ce type sont en effet hébergées sur de faux sites web. Il suffit donc à l'authentificateur de comparer les noms de domaine à ceux enregistrés à l'étape 3.



Exemple d'attaque par phishing

Après réception de la demande d'authentification, l'authentificateur vérifie le nom de son domaine d'origine. Comme illustré ci-dessus, les attaques par phishing classiques redirigent généralement l'utilisateur vers un faux site où il doit indiquer ses identifiants, qui sont ensuite détournés pour pirater des comptes. Avec WebAuthn, ce risque est tout simplement exclu, puisque l'authentificateur (dans ce cas précis, un smartphone) vérifie le nom de domaine pour l'utilisateur. Cette procédure évite tout risque d'erreur humaine, en l'occurrence la saisie d'identifiants sur un site malveillant.

Principe de fonctionnement de la récupération de comptes

Si vous perdez votre terminal, vous ne pouvez plus vous en servir pour vous authentifier dans votre instance via WebAuthn. Il est donc indispensable de prévoir d'autres facteurs, ainsi qu'un dispositif de récupération. Voici quelques exemples de facteurs pris en charge par Okta :

Okta Verify	SMS Auth	Google Auth	Windows Hello
U2F (FIDO 1.0)	YubiKey	Duo Security	Symantec VIP
On-Prem MFA	RSA SecurID	Security Question	Voice Call Auth

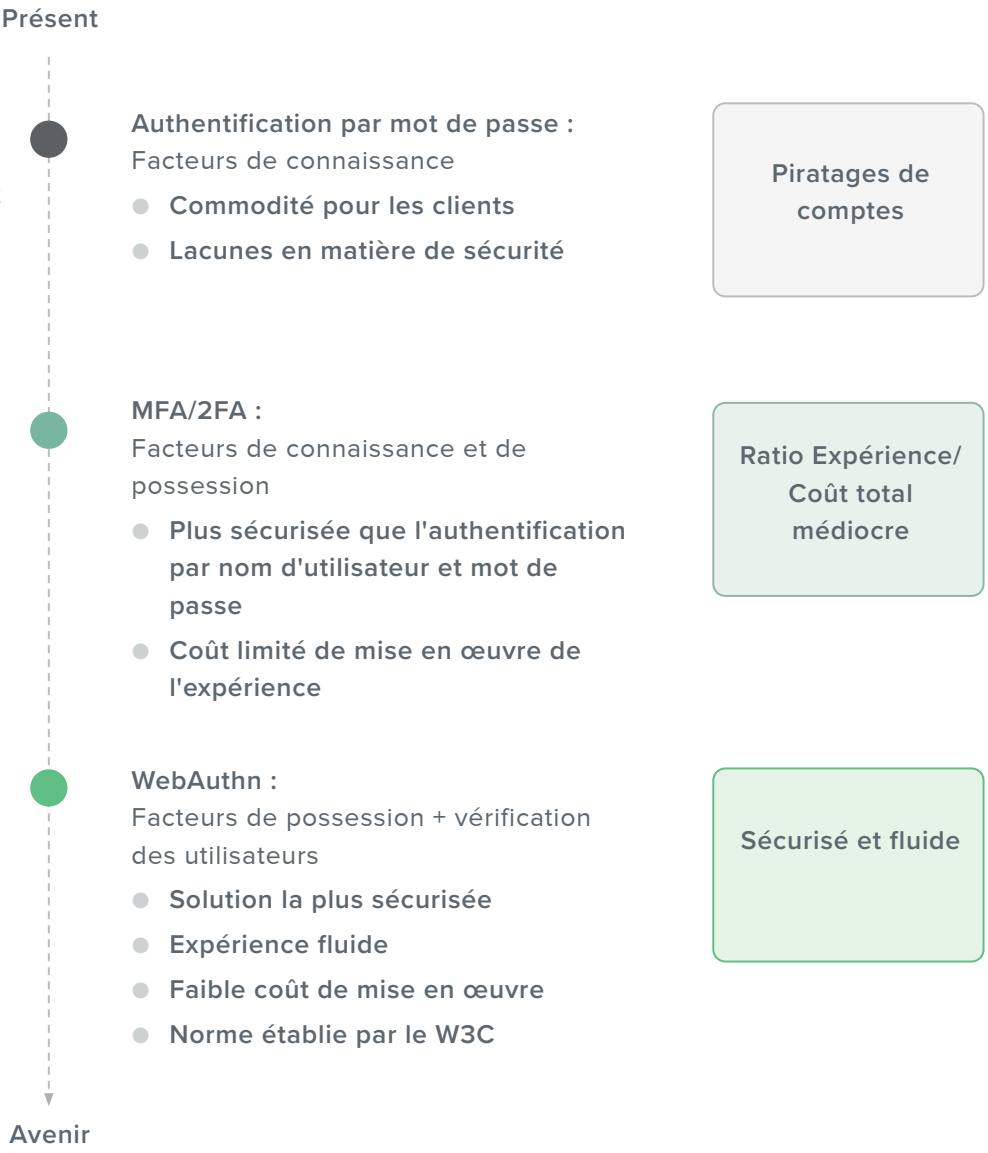
Bonnes pratiques d'Okta

Le niveau de protection réel d'une entreprise est celui du maillon le plus faible dans la chaîne de sécurité. Pour limiter les risques si vous n'avez prévu aucun de ces facteurs, offrir davantage de visibilité permet de s'assurer que les incidents suspects sont immédiatement signalés et pris en compte. Cela passe notamment par l'envoi automatique d'e-mails ou de notifications informant l'utilisateur qu'une récupération de facteur ou de mot de passe est demandée.

4e partie : Vers un avenir sans mot de passe

Avec ces nouvelles utilisations de WebAuthn, les entreprises peuvent envisager un monde plus sûr, sans mots de passe. Chez Okta, notre objectif est de développer des solutions pour aider nos clients à relever les défis de l'authentification. Nous nous engageons également à prendre en charge les normes d'authentification comme WebAuthn, qui facilitent l'adoption de stratégies passwordless à plus grande échelle.

Grâce à cette nouvelle norme, des problèmes tels que le piratage de comptes et l'expérience utilisateur médiocre appartiendront bientôt au passé.



Okta propose différents produits pour aider les entreprises à renforcer leur sécurité. Les déficiences des systèmes d'authentification se sont soldées par une multiplication des attaques d'usurpation d'identité, et notre solution Okta Adaptive Multi-Factor Authentication est conçue pour réduire ces risques et en limiter l'impact sur l'utilisateur.

Pour en savoir plus sur les spécifications techniques de WebAuthn, consultez la page WebAuthn du W3C.

Autres liens Okta utiles

It's a New World with WebAuthn: Passwordless Authentication Goes Primetime

WebAuthn: A Developer's Guide to What's on the Horizon

WebAuthn, the Road to Passwordless, and Other Considerations

How FIDO2 + WebAuthn Offer a Seamless, Secure Login

Qui sommes-nous ?

Okta est la première société indépendante spécialisée dans la gestion et la protection des données d'identification. Conçue pour les professionnels, la solution Okta Identity Cloud permet de connecter en temps et en heure et de façon sécurisée les utilisateurs aux technologies dont ils ont besoin. Dans un souci de simplicité, nous proposons plus de 6 000 intégrations clés en main pour les applications et les fournisseurs d'infrastructures. Nos clients peuvent ainsi profiter en toute sécurité des technologies les mieux adaptées à leur activité. Plus de 6 100 entreprises nous font confiance pour les aider à protéger les données d'identification de leurs employés et de leurs clients. Parmi celles-ci, on retrouve notamment 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America ou encore Twilio.

www.okta.com/fr