OTP OTC OTL

Quoi et quand les utiliser ?

Diawando DIAWARA
PETIT CŒUR TECHNOLOGIE SARL

Table des matières

Introduction :..... 2
Cas d'utilisation de la méthode d'authentification par possession : 2
OTP : 2
Avantages : 3
Inconvénients : 3
OTC : 3
Cas d'utilisation : 3
Avantages : 3
Inconvénients : 4
OTL :..... 4
Cas d'utilisation : 4
Avantages : 4
Inconvénients : 4
Conclusion : 5
Bibliographie :..... 6

Introduction :

Face aux défis constants de garantir aux utilisateurs un accès sécurisé aux plateformes numériques et à leurs données, plusieurs méthodes d'accès sécurisé ont vu le jour. A savoir trois principales :

- L'authentification par connaissance ;
- L'authentification par possession (celle que nous aborderons brièvement) ;
- Et l'authentification par inhérence.

Les cyberattaques comme le phishing, les attaques par force brute et le piratage de comptes représentent des menaces majeures pour la sécurité des utilisateurs. Afin de répondre à ces défis, des mécanismes d'authentification et de vérification robuste ont été développés pour protéger les accès aux plateformes numériques. Parmi ces mécanismes, les méthodes basées sur la possession (Authentification par possession) telles que l'OTP, l'OTC, et l'OTL se sont imposées comme solutions efficaces.

Bien que ces trois acronymes soient souvent confondus, ils désignent des mécanismes d'authentification légèrement différents, chacun ayant ses propres caractéristiques et cas d'utilisations.

Bien avant d'aborder ces trois mécanismes et leurs spécificités, je vais répondre à la question de savoir ce qu'est la méthode d'authentification par possession.

Authentification par possession :

La méthode d'authentification par possession repose sur l'utilisation d'objet physique ou numérique que seul l'utilisateur possède, comme une clé USB sécurisée, un smartphone ou une carte à puce.

Cas d'utilisation de la méthode d'authentification par possession :
Cette méthode peut être utilisée dans les contextes suivants :

- Authentification à deux facteurs (2FA) via SMS ou application d'authentification (google authenticator)
- Connexion à des systèmes sécurisés avec une clé de sécurité (Yubikey)
- Validation de transactions bancaires via un code OTP.

OTP :

L'OTP ou One Time Password est un mot de passe temporaire, valable pour une courte durée (quelques secondes à quelques minutes), et à usage unique, valable pour une seule session ou transaction.

Généré automatiquement, il est généralement envoyé via des canaux sécurisés comme les SMS ou des applications d'authentification.

Cas d'utilisation :

- Connexion à des système sécurisés : Certaines entreprises utilisent des OTP pour permettre à leurs personnels d'accéder à des systèmes internes.
- Authentification à double facteurs (2FA) : Lors de la connexion à une application en ligne (Banque, Cloud public), après avoir entré vos identifiant et mot de passe principal, l'application vous envoie un OTP par SMS, par mail ou via une application d'authentification (comme Google Authenticator).
- Validation de transactions : Après un achat sur un site en ligne avec votre Carte Visa, un OTP peut être envoyé pour confirmer que vous êtes bien à l'origine de la transaction.

Avantages :

- Réduit les risques de réutilisation, car le code expire rapidement.
- En cas de vol de mot de passe, une seconde barrière reste à franchir pour accéder à vos données.

Inconvénients :

- Dépend de la disponibilité du réseau pour la réception des SMS ou emails.
- Vulnérable aux attaques telles que le SIM swapping, où un attaquant obtient le contrôle de la carte SIM de la victime et intercepte les OTP envoyés par SMS.

OTC :

L'OTC est un code temporaire à usage unique, plus flexible qu'un OTP, pouvant contenir des lettres et des chiffres. Souvent utilisé pour authentifier des actions spécifiques (comme une connexion ou une transaction).

Il peut être envoyé via différents canaux SMS, Email.

Cas d'utilisation :

- Les OTC sont fréquemment utilisés pour vérifier l'identité ou confirmer une action sensible, souvent lors de la première connexion depuis un nouvel appareil ou pour la récupération de compte.
- Inscription à un service : Lorsque vous créez un compte sur une plateforme, un OTC peut être envoyé pour vérifier votre adresse e-mail ou votre numéro de téléphone.
  Récupération de compte : Si vous oubliez votre mot de passe, un OTC peut être envoyé pour réinitialiser vos informations d'identification.
- Validation d'un coupon : Un OTC peut être utilisé pour activer une offre spéciale ou un coupon de réduction.

Avantages :

- Peut être utilisé dans de multiples scénarios de sécurité (authentification, vérification de l'identité, etc.).

Inconvénients :

- Comme l'OTP, il peut être intercepté s'il est envoyé via des canaux non sécurisés (ex : email)

OTL :

L'OTL est un lien (URL) à usage unique et temporaire, avec une durée de vie généralement plus longue que celle des OTP et OTC.

Il permet à un utilisateur d'accomplir une action spécifique (par exemple, se connecter ou réinitialiser un mot de passe) sans avoir à saisir de code. L'utilisateur reçoit un lien par email ou SMS qu'il doit simplement cliquer pour être redirigé vers une page sécurisée. Ce lien expire après son utilisation ou après un certain temps.

Cas d'utilisation :

- Réinitialisation de mot de passe : Lorsqu'un utilisateur demande une réinitialisation de son mot de passe, un lien à usage unique est envoyé à son adresse email, en cliquant sur ce lien, il peut directement accéder à une page pour créer un nouveau mot de passe.
- Validation d'un compte : Lorsqu'un utilisateur s'inscrit à un service, un OTL peut être envoyé pour confirmer son adresse e-mail. Cliquer sur le lien valide son compte.
- Téléchargement de fichiers confidentiels : un OTL peut être utilisé pour partager un fichier ou une ressource de manière sécurisée, par l'envoie d'un lien à usage unique pour le téléchargement.

Avantages :

- Très convivial, car l'utilisateur n'a pas besoin de se souvenir d'un mot de passe ou de saisir un code.
- Utile pour des actions rapides (connexion instantanée, réinitialisation)

Inconvénients :

- S'il l'email de l'utilisateur est compromis, un attaquant pourrait utiliser l'OTL pour accéder au compte
- Moins sécurisé si des mesures comme l'expiration rapide du lien ne sont pas mises en place.

Pour finir voici un tableau comparatif de chacune des méthodes :

Aspect	OTP (One Time Password)	OTC (One Time Code)	OTL (One Time Link)
Format	Code numérique (ex : 123456)	Code alphanumérique (ex : ABC123)	Lien URL (ex : htt://...)
Durée de validité	Court (généralement en quelques secondes/minutes)	Expire après utilisation ou un certain délai (selon le contexte)	Expire après utilisation ou un certain délai (selon le contexte)
Cas d'utilisation	Authentification, Transactions	Vérification, récupération	Confirmation, accès unique
Support	SMS, app d'authentification	SMS, e-mail	E-mail
Sécurité	Forte (mais dépend du canal utilisé)	Forte (mais dépend du canal utilisé)	Moyenne (risque si email compromis)
Mise en œuvre	Modérément complexe, nécessite une infrastructure pour générer et envoyer des OTP	Simple, car il peut être intégré via des solutions existantes comme les API d'authentification par email ou SMS	Complexe, car il nécessite la gestion des URLS temporaires et des liens sécurisés
Coût associés	Frais lié à l'envoi de SMS	Moins coûteux, s'il est envoyé par email	Faible côut d'envoi, mais peut nécessiter un stockage sécurisé des liens

Conclusion :

Les méthodes d'authentification par possession, telles que l'OTP, l'OTC et l'OTL, jouent un rôle crucial dans la sécurisation des accès aux plateformes numériques. Chacune de ces méthodes a ses propres caractéristiques et cas d'utilisation, ce qui les rend adaptées à des contextes spécifiques. L'OTP est idéal pour les authentifications à deux facteurs, l'OTC pour les vérifications ponctuelles, et l'OTL pour les actions nécessitant un clic unique. Le choix de la méthode dépend des besoins de sécurité, de l'expérience utilisateur et des contraintes techniques. Dans un monde où les cybermenaces sont de plus en plus sophistiquées, il essentiel de comprendre et d'utiliser ces outils de manière appropriée pour protéger les données et les systèmes.

Bibliographie :

Descope.com *(What Are Magic Links and How Do They Work ?)*

RFC 6238 (*TOTP: Time-Based One-Time Password Algorithm)*

RFC 4226 *(HOTP: An HMAC-Based One-Time Password Algorithm)*

Clerk.com *(Ultimate Guide to Magic Link Authentication)*

Onelogin.com *(HOTP ? Understanding the different types of OTP and where an OTP generator fits in)*