Les jetons individuels de connexion ou token access

08 septembre 2022

Mécanisme fréquemment intégré aux procédures d'authentification, le jeton individuel d'accès (*token access*) permet une connexion sécurisée à un espace personnel, un compte ou encore des documents bureautiques. La CNIL fait le point sur ses usages, ses enjeux et les bonnes pratiques à appliquer.

L'authentification par jeton d'accès

L'authentification par jeton est une **forme d'authentification** qui permet à un utilisateur d'accéder à un service en ligne, une application, ou un site web sans qu'il n'ait à ressaisir ses identifiants. Par conséquent, grâce à cette forme d'authentification, l'utilisateur pourra accéder à ses ressources en ligne, au moyen de ce **jeton d'accès,** tant qu'il reste valide.

Par ailleurs, les jetons sont également souvent utilisés dans une procédure d'authentification à double facteur afin de réduire les risques d'usurpation de comptes. Dans ce cas, à l'ouverture d'une session de connexion par identifiant et mot de passe, un jeton d'accès est transmis à l'utilisateur afin de confirmer son identité.

Si les jetons sont parfois des jetons physiques de longue durée (qui peuvent être quelque chose « que l'on possède » — comme des clés, disques, carte à puce — ou « que l'on est », comme une identification biométrique), ils sont plus souvent des **jetons numériques ou dématérialisés**, transmis par un serveur vers un terminal et qui ont généralement une durée de validité limitée. Il peut alors s'agir d'un code ou d'un lien contenant un jeton alphanumérique, transmis par SMS ou courrier électronique.

Dans le cadre de cet article, la CNIL n'aborde que l'authentification à distance par jeton numérique, qui est la technique la plus répandue.

Usages courants du jeton numérique

L'authentification par jeton numérique s'est fortement généralisée ces dernières années et est fréquemment mise en œuvre pour :

- les procédures de confirmation de création de compte, de génération et de renouvellement de mot de passe ;
- **la connexion automatisée** à un serveur pour faciliter l'accès à un service donné :
  - panier enregistré lors d'un parcours d'achat et accessible par un lien envoyé par courriel ;
  - validation d'un formulaire pour le recueil du consentement ;
  - pages de désinscription à des lettres d'information ;
- **la consultation directe** de documents et de données en ligne par la transmission d'un lien avec un jeton à l'utilisateur ou à un robot pour qu'il puisse accéder à des documents ou des informations tels que :
  - des bons de livraison ;
  - des documents bureautiques en ligne ;
  - des résultats d'examens médicaux ;
  - ou d'autres données, comme les résultats d'une requête transmise à une interface de programmation d'application.

Dans tous ces cas, le serveur émet à l'utilisateur un lien à suivre incluant un jeton d'authentification : lorsque l'utilisateur clique sur ce lien, le serveur vérifie la validité du jeton, accepte l'authentification et active la fonctionnalité demandée par l'utilisateur.

Menaces et risques

Un jeton d'accès, matérialisé sous la forme de lien, peut être considéré comme un moyen d'accès continu à des données personnelles accessibles depuis Internet. Cette « porte d'entrée » est, en soi, une vulnérabilité dont le risque en matière de sécurité doit être pris en compte.

En effet, le jeton d'accès, s'il est transmis/accessible à des tiers qui n'ont pas à le connaître ou fait l'objet d'une interception par des acteurs malveillants, peut entraîner la compromission de l'intégrité ou la confidentialité de données personnelles (par exemple dans le cas de documents bureautiques partagés ou de bons de livraison), de comptes utilisateurs ou encore d'espaces personnels en ligne.

Dans ces conditions, il est nécessaire de mettre en œuvre des contre-mesures afin d'éviter l'accès non autorisé à des données personnelles.

Attention aux risques d'hameçonnage

L'envoi de jetons frauduleux par courriel ou SMS est devenu une pratique d'hameçonnage (ou *phishing* en anglais) qui s'est largement développée et qui permet à des attaquants d'obtenir des renseignements

personnels qui peuvent ensuite leur permettre d'usurper l'identité de la victime.

Face à la multiplication de ces arnaques, les sites utilisant des jetons de manière légitime ont intérêt à **sensibiliser leurs utilisateurs sur ces risques** et à **les informer sur leur usage de jetons**.

Préconisations générales

En l'absence d'authentification à double facteur, le jeton individuel de connexion à distance entraîne un risque accru en matière de sécurité, ce que la CNIL a pu constater lors de ses contrôles au cours de ces derniers mois.

Les risques liés à l'utilisation du jeton d'accès sont nombreux et variés mais certains principes permettent de réduire la probabilité qu'ils surviennent :

- Journaliser la création et l'utilisation des jetons.
- **Définir une durée de validité** aux jetons, adaptée aux finalités (ou objectifs – voir les exemples pratiques ci-dessous).
- **Générer un lien d'authentification ne contenant aucune donnée personnelle** ou des variables au contenu facilement compréhensible et réexploitable, comme un contenu haché.
- **Imposer une nouvelle authentification** (par identifiant et mot de passe, par exemple) dans le cas où le jeton permet l'accès à des données personnelles ou si le jeton a une durée de vie insuffisamment limitée.
- **Limiter le nombre d'accès** comme l'usage unique ou temporaire en fonction des finalités visées. Dans le cadre d'un transfert de données entre deux services, l'utilisation d'un jeton d'accès pour établir la connexion entre les deux services doit également être limitée dans le temps.
- **Restreindre l'utilisation du jeton à certains services ou ressources** en évitant sa réutilisation pour tous les parcours utilisateurs. Dans le cadre d'une confirmation de création de comptes, ne pas autoriser également une authentification automatique au compte utilisateur qui lui permettrait d'accéder à toutes ses données, ses commandes, etc.
- **Supprimer automatiquement, de manière temporaire ou définitive,** l'accès à la ressource demandée en cas de demandes intensives suspecte.
- **Permettre la révocation d'un jeton** depuis un compte utilisateur ou en cas de comportement suspect automatiquement détecté.

En fonction de la nature des services et des ressources demandées, les utilisateurs devraient pouvoir choisir les modalités de transmission de leur de jeton d'accès à distance. Cela concerne notamment :

- **le mode d'expédition** du jeton : courriel, SMS, envoi postal, appel téléphonique ;
- **le mode de notification** à l'utilisateur de l'usage d'un jeton.

Trois exemples pratiques de jetons individuels de connexion

- **Confirmation de la création d'un compte utilisateur**

Afin de confirmer la création d'un compte ou d'un espace personnel, un lien est généralement transmis à un utilisateur pour vérifier qu'il est bien propriétaire de l'adresse électronique qu'il a renseignée. Dans ce cas, il est recommandé de suivre les étapes suivantes pour une mise en œuvre sécurisée :

1. L'action de vérification devant suivre la demande de création de comptes, **la durée du jeton délivré ne doit pas excéder quelques minutes** ;
2. Après conformation de l'identité de l'utilisateur via le suivi du lien, **le jeton d'accès ne doit pas permettre à l'utilisateur de se connecter automatiquement à son compte**. Il devra s'authentifier à partir des identifiants du compte pour accéder aux fonctionnalités de l'application ou des services en ligne ;
3. **Transmettre une notification à l'utilisateur** (courriel ou SMS) afin de confirmer la validité de son adresse électronique et de la création de son compte.

- **Suivi de livraison**

Dans le cadre du suivi de livraison postale, il est possible de proposer aux destinataires un accès simplifié par lien direct. Dans ce cas, le numéro d'identifiant de l'expédition peut être utilisé comme jeton dans le lien d'accès à la page de suivi de la livraison.

Toutefois, l'affichage de données personnelles liées à l'expéditeur ou au destinataire, comme leur identité et leur adresse postale, doit être absent de cette page.

La durée du jeton ne doit pas excéder quelques jours après que la livraison postale ait été effectuée.

- **Échange de fichiers**

Enfin, pour les plateformes d'échange de fichiers, le jeton d'authentification peut avoir un nombre d'utilisations limité afin de permettre à l'utilisateur de pouvoir utiliser cette connexion automatique et télécharger les fichiers nécessaires sans toutefois introduire une vulnérabilité qui permettrait à un tiers de les télécharger ultérieurement.

Si les fichiers doivent être accessibles par plusieurs destinataires, un jeton différent doit être transmis à chaque destinataire.

Dans la mesure où l'échange de fichiers revêt un caractère ponctuel, **la durée du jeton ne doit pas excéder quelques jours** après que les fichiers aient été transmis.

Texte reference

Pour approfondir

> Sécurité : authentifier les utilisateurs
> Utilisez l'authentification multifacteur pour vos comptes en ligne
> Smartphone : authentification avec vos données biométriques
Haut de page