Mes clés numériques Version 4.0 –02/03/2021

CSAM

CONDITIONS D'UTILISATION « MES CLÉS NUMÉRIQUES - S'IDENTIFIER À L'ADMINISTRATION EN LIGNE »

Article 1er - Champ d'application des présentes conditions d'utilisation

Les présentes conditions d'utilisation règlent la procédure mise en place par l'Administration fédérale pour l'enregistrement, l'identification et l'authentification électroniques d'utilisateurs finaux, citoyens ou non. Par le biais de cette procédure, les utilisateurs finaux peuvent s'enregistrer afin d'accéder de manière sécurisée à des services électroniques de l'Administration et de communiquer électroniquement en toute sécurité avec l'Administration.

Il se peut cependant que certaines instances publiques aient recours à d'autres systèmes de gestion électronique des utilisateurs finaux.

Article 2 - Accès à la procédure

L'utilisateur final a accès à la procédure sans que l'on puisse cependant lui garantir que l'accès à la procédure et les services offerts seront en tout temps assurés, ne présenteront aucunes erreurs et ne seront pas perturbés techniquement.
L'accès à la procédure peut, à tout moment, être partiellement ou entièrement bloqué (notamment à des fins de maintenance). Pour autant que ce soit raisonnablement possible, l'utilisateur final sera préalablement tenu informé de telles interruptions.
L'utilisateur final n'aura accès à certains services offerts par l'Administration qu'après avoir suivi la procédure d'enregistrement, d'identification et d'authentification applicable.
Dans ce cadre, l'utilisateur final devra :

- marquer son accord sur les présentes conditions d'utilisation ;
- communiquer une adresse e-mail correcte .

Si nécessaire, l'utilisateur final est tenu d'adapter les données le concernant afin qu'elles soient toujours actualisées et correctes.

Article 3 - Utilisation de clés numériques

L'accès de l'utilisateur final à certains services offerts par voie électronique nécessite l'utilisation de clés numériques (eID, code de sécurité via application mobile/SMS/email et nom d'utilisateur et mot de passe…).

Certaines clés numériques sont entièrement offertes par la DG Transformation digitale du SPF Stratégie et Appui et d'autres le sont par des parties agréées par la DG Transformation digitale du SPF Stratégie et Appui. Un tel agrément ne peut être octroyé que moyennant le respect, notamment, d'exigences strictes relatives à la sécurité et à la vie privée prévues dans l'Arrêté royal du 22 octobre 2017 fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques numériques.

Ces clés numériques, ainsi que les données qui y sont liées, sont strictement personnelles et non transmissibles.
Chaque utilisateur final est responsable de la bonne conservation, sécurisation, discrétion et gestion de ses clés numériques et des données qui y sont associées.
L'utilisateur final est responsable du choix d'un mot de passe ou autre code secret sûr.

Si un utilisateur final a connaissance de la perte de son nom d'utilisateur, mot de passe, ou de toute autre clé numérique, ou de leur utilisation illicite par des tiers, ou s'il soupçonne une telle perte ou une telle utilisation illicite, il doit immédiatement prendre toutes les mesures nécessaires afin de désactiver la clé numérique comme prescrit à l'article 6 notamment.
En cas de verrouillage de sa clé numérique, l'utilisateur final devra en demander une nouvelle.

Article 4 - Utilisation de l'adresse e-mail

L'utilisateur final est responsable du choix de l'adresse e-mail qu'il a communiquée. Il déclare que cette adresse e-mail lui appartient et que des tiers ne peuvent en faire usage sans son autorisation.

L'utilisateur final confirme utiliser régulièrement cette adresse.

Article 5 - Utilisation de la procédure

Chaque utilisateur final est tenu de :
1. fournir des informations complètes, précises, véridiques et non mensongères ;
2. respecter les dispositions prescrites par voie de loi, règlement, décret, ordonnance ou arrêté de l'autorité fédérale, régionale, locale ou internationale ;
3. s'abstenir de manipuler les informations fournies, de quelque manière que ce soit et avec quelque technique que ce soit.

Article 6 - Procédure en cas de perte ou de modification d'une (partie d'une) clé numérique

En cas de perte ou de vol d'une carte d'identité, son titulaire est tenu d'en faire la déclaration au plus vite au service de la Population de sa commune ou au poste de police le plus proche, ou de prendre contact avec le service DocStop du SPF Intérieur.

Si un utilisateur final perd son smartphone ou son GSM, ou se le fait voler, il est tenu de le signaler au plus vite à son fournisseur de services. Il doit par ailleurs supprimer dans « Mes clés numériques » les clés en question (code de sécurité via application mobile et/ou code de sécurité via SMS et/ou code de sécurité via email).

Si un utilisateur final souhaite utiliser un nouveau numéro de GSM, il est tenu de supprimer au préalable dans « Mes clés numériques » la clé « code de sécurité via SMS » pour l'ancien numéro.

Lorsqu'un utilisateur final a perdu son token, il doit le désactiver. L'ancien token sera immédiatement désactivé et ne sera plus utilisable à partir de ce moment-là.

Article 7 - Protection de la vie privée

L'Administration veille à votre vie privée et, dans ce cadre, agit toujours conformément aux dispositions de la législation belge et européenne en matière de protection des données.
Vous pouvez consulter notre déclaration de confidentialité ici.

Article 8 - Définitions

Aux fins des présentes conditions d'utilisation, les notions ci-dessous sont définies comme suit :

- **Enregistrement** - Le processus par lequel une personne se fait inscrire - en suivant une procédure préétablie - dans une liste, et donne dès lors à connaître qu'elle souhaite faire usage d'un certain service.
- **Identification** - Un processus qui est utilisé pour constater l'identité d'une certaine personne.

- **Authentification** - Processus utilisé pour confirmer l'identité d'une certaine personne. Une personne peut par exemple, en fournissant certaines données confidentielles qui ne sont connues que d'elle (p. ex. un mot de passe choisi par elle-même), confirmer qu'elle est bel et bien la personne qu'elle prétend être.