

Règlement à l'usage des utilisateurs en vue de l'accès et de l'utilisation du système informatique de l'Etat fédéral et des institutions publiques de sécurité sociale par les citoyens et leurs mandataires

Article 1er - Champ d'application

Ce règlement à l'usage des utilisateurs régit l'accès au système informatique de l'Etat fédéral et des institutions publiques de sécurité sociale (appelé ci-après système d'information) et son utilisation par les citoyens et leurs mandataires, en ce compris les services que ce système dispense.

Article 2 –Définition

Par « carte d'identité électronique » au sens du présent règlement, il y a lieu d'entendre la carte d'identité électronique, visée par les articles 6 et suivants de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, sur laquelle les certificats d'identité et de signature sont activés.

Article 3 - Services dispensés et canaux disponibles

Les services dispensés sont accessibles par différentes voies :

1. Via le site-portal de la sécurité sociale (www.securitesociale.be)
 - a) tous les utilisateurs ont accès aux applications reprises dans le tableau de l' « ANNEXE 1 – Applications via le site-portal de la sécurité sociale » ;
 - b) l'accès à ces applications peut requérir l'utilisation d'une clé numérique. Un niveau de fiabilité est associé à chacune de ces clés numériques. Si ce niveau est suffisant pour l'accès à une application, ceci vaut également pour les autres clés numériques appartenant au même niveau ou à un niveau supérieur. Le tableau indique, par application, quelles sont les clés numériques dont le niveau est suffisant. Les nouvelles clés numériques futures pourront être utilisées immédiatement, conformément à leur niveau de fiabilité.
2. Via le site-portal de l'autorité fédérale (www.belgium.be)
 - a) tous les utilisateurs ont accès aux applications reprises dans le tableau de l' « ANNEXE 2 – Applications via le site-portal de l'autorité fédérale »;
 - b) l'accès à ces applications peut requérir l'utilisation d'une clé numérique. Un niveau de fiabilité est associé à chacune de ces clés numériques. Si ce niveau est suffisant pour l'accès à une application, ceci vaut également pour les autres clés numériques appartenant au même niveau ou à un niveau supérieur. Le tableau indique, par application, quelles sont les clés numériques dont le niveau est suffisant. Les nouvelles

clés numériques futures pourront être utilisées immédiatement, conformément à leur niveau de fiabilité.

3. Via le portail eSanté (www.ehealth.fgov.be)

- a) tous les utilisateurs ont accès aux applications reprises dans le tableau de l' « ANNEXE 3 – Applications via le site-portail eSanté »;
- b) l'accès à ces applications peut requérir l'utilisation d'une clé numérique. Un niveau de fiabilité est associé à chacune de ces clés numériques. Si ce niveau est suffisant pour l'accès à une application, ceci vaut également pour les autres clés numériques appartenant au même niveau ou à un niveau supérieur. Le tableau indique, par application, quelles sont les clés numériques dont le niveau est suffisant. Les nouvelles clés numériques futures pourront être utilisées immédiatement, conformément à leur niveau de fiabilité.

La teneur des services et l'accès à ces services peuvent être modifiés à tout moment.

Article 4 – Accès au système d'information

L'utilisateur a accès au système d'information, sans qu'il soit pour autant garanti que cet accès et celui aux services offerts soient assurés en tout temps et qu'ils ne soient entachés d'aucune erreur ou ne s'accompagnent d'éventuelles difficultés techniques.

L'accès au système d'information et aux services dispensés par le biais du système peut, à tout moment, être complètement ou partiellement interrompu (notamment pour des raisons d'entretien). Dans les limites du raisonnable, l'utilisateur sera informé préalablement d'une telle interruption.

L'utilisateur est responsable de la mise à disposition et de la maintenance du terminal nécessaire à l'utilisation du système d'information. Les fournisseurs d'accès du système d'information ne sont pas responsables du terminal, ni de l'utilisation qui en est faite et ils ne sont pas tenus d'en assurer le support, sous quelque forme que ce soit.

Article 5 – Utilisation des clés numériques

L'accès de l'utilisateur à certains services offerts par la voie électronique nécessite l'utilisation de clés numériques (par exemple, lecteur de cartes eID, code de sécurité sur base du TOTP (Time-based One-time password) via application mobile ou SMS, token de citoyen et nom d'utilisateur et mot de passe, clés (mobiles) offertes dans le cadre de services agréés conformément à l'AR du 22 octobre 2017 fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques).

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, token de citoyen, 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.

En cas de verrouillage de sa clé numérique, l'utilisateur final devra en demander une nouvelle.

Les clés numériques sont utilisées dans le cadre de CSAM (voir <https://www.csam.be/>). La création et l'utilisation de celles-ci sont aussi réglées dans la convention d'utilisation de CSAM. Certaines clés numériques ne sont pas disponibles pour chaque application.

Article 6 – Utilisation du système d'information

En ce qui concerne l'utilisation du système d'information et des services dispensés via ce système, chaque utilisateur :

1. doit fournir des informations qui sont complètes, exactes et véritables et qui ne sont pas susceptibles d'induire en erreur;
2. doit respecter les dispositions prescrites par voie de loi, de règlement, de décret, d'ordonnance ou d'arrêté pris par les instances fédérales, régionales, locales ou internationales;
3. doit s'abstenir de manipuler les informations fournies, et ce de quelque manière que ce soit ou en recourant à une technique quelconque;
4. ne peut, via le système d'information, envoyer aucune donnée, ni avis, ni document, de quelque manière que ce soit, ni charger des données ou des documents par ce biais :
 - a) opérations qui porteraient atteinte aux droits (dont les droits de la personnalité ou de la propriété intellectuelle) de tiers ou des fournisseurs du système d'information;
 - b) dont le contenu est illicite, source de dommages, diffamatoire, violent, obscène ou déshonorant ou qui porte atteinte à la vie privée de tiers;
 - c) dont l'utilisation ou la possession par l'utilisateur est interdite par la loi ou par convention;
 - d) qui contiennent des virus ou des instructions susceptibles de causer des dommages aux fournisseurs du système d'information et/ou au système d'information et qui pourraient mettre en péril ou perturber les services dispensés par le biais du système d'information.

Article 7 – Utilisation des certificats de la carte d'identité électronique

L'accès de l'utilisateur à certains services suppose l'utilisation d'une carte d'identité électronique. Dans l'hypothèse de l'accès aux services dispensés via une carte d'identité électronique, l'authentification est réalisée par le certificat d'identité de la carte et la signature électronique est apposée via le certificat de signature de la carte.

Dès le moment de la création de la clé privée, le titulaire du certificat est seul responsable de sa confidentialité. En cas de doute quant au maintien de la confidentialité de la clé privée ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat. Lorsqu'un certificat est arrivé à échéance ou a été révoqué,

le titulaire de celui-ci ne peut, après l'expiration du certificat ou après révocation, plus utiliser la clé privée correspondante pour signer ou faire certifier ces données par un autre prestataire de service de certification.

Tout utilisateur doit donc user judicieusement de la clé privée et du certificat ainsi que du mot de passe éventuel nécessaire à l'utilisation de la clé privée et du certificat. L'utilisateur est responsable de tout usage approprié ou non de la clé et du certificat, en ce compris toute utilisation par des tiers.

Article 8 – Utilisation des signatures électroniques et justification

Les messages envoyés via le système d'information par l'utilisateur en utilisant le certificat de signature de la carte d'identité électronique sont accompagnés d'une signature électronique visée à l'article 1322, alinéa 2, du Code civil.

L'utilisateur reconnaît expressément que tous les messages qui sont envoyés via le Système d'information et qui sont accompagnés d'une signature électronique ont la même force probante qu'un acte sous seing privé au sens du Code civil.

L'utilisateur reconnaît expressément que toutes les informations relatives à des messages et sauvegardées par les fournisseurs du système d'information de manière durable et sans qu'elles ne puissent être modifiées, ont la même force probante qu'un acte sous seing privé au sens du Code civil, et ce jusqu'à preuve du contraire.

L'utilisateur reconnaît expressément comme étant la sienne la signature qui a été apposée sur la base de sa carte d'identité électronique, sauf en cas d'abus, de perte ou de vol, pour autant que la procédure spécialement prévue à cet effet ait été respectée.

Article 9 – Obligation de contrôle de l'utilisateur

L'utilisateur est responsable du contrôle du contenu des messages qu'il a envoyés par le système d'information et de leur suivi dans le cadre des messages qui sont transmis par les fournisseurs du système d'information à l'utilisateur et qui ont trait au(x) message(s) envoyé(s) par l'utilisateur.

L'erreur (les erreurs) matérielle(s) contenue(s) dans un message envoyé par l'utilisateur, dans un accusé de réception y afférent ou dans tout autre message ou document qui a trait à l'utilisateur et qui est accessible par le système d'information, est (sont) rectifiée(s) à la demande de l'utilisateur par le biais d'une procédure de rectification prévue à cet effet.

Article 10 – Propriétés intellectuelles

L'utilisateur reconnaît et accepte que le système d'information et les services ainsi que le logiciel développé pour ce système d'information et ces services sont protégés par des droits en matière de propriété intellectuelle (droits d'auteur, droit des marques, droit de brevet, etc.) qui appartiennent aux fournisseurs du système d'information (ou à leurs fournisseurs de brevet).

L'utilisateur bénéficie du droit non-exclusif d'utiliser le système d'information aux fins stipulées dans le règlement à l'usage des utilisateurs. Sauf autorisation expresse, il est interdit à l'utilisateur de copier de quelque manière que ce soit ou sur un quelconque support, tout ou partie du système d'information, de l'adapter, de le traduire, de le donner en location, de le prêter, de le communiquer au public et de créer des travaux dérivés des éléments susvisés.

ANNEXE 1 - Applications via le site-portal de la sécurité sociale

Application	UID/PWD	Token avec UID/PWD	eID ITSME X509 cert. TOTP (App ou SMS)
	+ futur	+ futur	+ futur
	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON
Calcul allocation de garantie de revenus	Pour ces applications, aucune clé numérique n'est requise		
Calcul du stage d'insertion professionnelle			
Mesure en faveur de l'emploi			
Simulation cotisation sociale indépendant			
Calculez vos allocations familiales			
Checkin at work	Oui	Oui	Oui
Carte de contrôle chômage complet (eC3)			
Carte de contrôle chômage complet (eC32)			
Fonds de fermeture des entreprises			
Interruption de carrière et crédit-temps			
Mon compte de vacances (consultation)			
Horeca@work - 50 days			
Interim@work	Non	Non	Oui
e-Box citoyen			
Demande de pension			
MyPension			
Ma pension complémentaire			
MyCareer			
Carte de contrôle chômage temporaire - eC32			
Mon dossier de chômage			
HANDIWEB			
Mesure en faveur de l'emploi			
Mon compte de vacances (modification)			
MyHandicap			
CEDRIC			
Student@work			

ANNEXE 2 - Applications via le site-portal de l'autorité fédérale

Application	UID/PWD	Token avec UID/PWD	eID ITSME X509 cert. TOTP (App) + futur
	+ futur	+ futur	+ futur
	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON
2003 - Elections	Pour ces applications, aucune clé numérique n'est requise		
2004 - Elections			
2007 - Résultats des élections fédérales			
Catalogue commun			
Payer avec des titres-services			
Réduction forfaitaire des tarifs énergétiques (Réduction Energie)	Oui	Oui	Oui
Police-on-web	Non	Oui	Oui
my.belgium.be			
Tax-on-web -dienst			

ANNEXE 3 - Applications via le site-portal eSanté

Application	UID/PWD + futur Niveau suffisant OUI/NON	Token avec UID/PWD + futur Niveau suffisant OUI/NON	eID ITSME X509 cert. TOTP (App) + futur Niveau suffisant OUI/NON
eTCT - Feed-back aux hôpitaux sur leurs prestations de soins et sur leur coût	Pour ces applications, aucune clé numérique n'est requise		
Source authentique dispositifs médicaux implantables			
Healthdata.be Data Reporting			
CEBAM Digital library for Health Platform Welzijn en Gezondheid	Oui	Oui	Oui
E-loket Zorg en Gezondheid	Non	Oui	Oui
Accréditation	Non	Non	Oui
Ma Santé			
Web Application Metahub			
eHealthConsent			
Moduledata-bank Jeugdhulp Vlaanderen			
Registre central de traçabilité			
Portail unique			