1er avril 2026

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 entreprises 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 entreprises et leurs mandataires, en ce compris les services que ce système dispense.

Article 2 – Désignation obligatoire d'un gestionnaire d'accès principal

Toute entreprise qui souhaite accéder au système d'information et l'utiliser doit désigner un seul et unique gestionnaire d'accès principal.

Article 2 bis - Définitions

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.

Par « gestionnaire d'accès » ou « gestionnaire local » au sens du présent règlement, il y a lieu d'entendre la ou les personne(s) physique(s), désignée(s) au sein de l'entreprise par la personne habilitée à cet effet, pour assurer la gestion des utilisateurs et des accès au niveau qui est le sien (le leur), qu'elle(s) agisse(nt) en qualité de gestionnaire d'accès principal, de co-gestionnaire d'accès principal, de (co-)gestionnaire d'accès ((co-)gestionnaire local).

Article 3 - Services dispensés et canaux disponibles

Les services dispensés sont accessibles par différentes voies :

1. Via le site-portail 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-portail de la sécurité sociale », telles qu'elles sont indiquées pour eux;

   b) chaque curateur qui est désigné en tant que gestionnaire d'accès (gestionnaire local) ou chaque utilisateur désigné par ce curateur a accès aux applications reprises dans le tableau de l'« ANNEXE 1 – Applications via le site-portail de la sécurité sociale », telles qu'elles sont indiquées pour lui;

   c) chaque utilisateur désigné par le gestionnaire d'accès principal d'une entreprise en tant que gestionnaire d'accès (gestionnaire local) a accès aux applications reprises dans le

tableau de l' « ANNEXE 1 - applications via le site-portail de la sécurité sociale », telles qu'elles sont indiquées pour lui;

d) chaque utilisateur qui est désigné par le gestionnaire d'accès (gestionnaire local) d'une entreprise a accès aux applications qu'il a été autorisé à utiliser par le gestionnaire d'accès (gestionnaire local) d'une entreprise, sans pour autant que cet accès puisse être plus large que celui réservé au gestionnaire d'accès (gestionnaire local) lui-même;

e) 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-portail 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-portail de l'autorité fédérale », telles qu'elles sont indiquées pour eux ;

b) chaque utilisateur désigné par une entreprise en tant que gestionnaire d'accès (gestionnaire local) a accès aux applications reprises dans le tableau de l' « ANNEXE 2 - applications via le site-portail de l'autorité fédérale », telles qu'elles sont indiquées pour lui;

c) chaque utilisateur qui est désigné par le gestionnaire d'accès (gestionnaire local) d'une entreprise et qui dispose du numéro du répertoire du mandant a accès aux applications reprises dans le tableau de l' « ANNEXE 2 - applications via le site-portail de l'autorité fédérale », telles qu'elles sont indiquées pour lui, et ce pour les personnes pour lesquelles il dispose d'un mandat afin d'utiliser ces applications pour leur compte et en leur nom et dont il a mis ce mandat à la disposition de la direction régionale des contributions directes compétente pour le bureau de taxation du mandant ;

d) chaque utilisateur qui est désigné par le gestionnaire d'accès (gestionnaire local) d'une entreprise et qui dispose, en ce qui concerne les applications mentionnées au point 3 c), du numéro du répertoire du mandant a accès aux applications qu'il a été autorisé à utiliser par le gestionnaire d'accès (gestionnaire local) d'une entreprise, sans pour autant que cet accès puisse être plus large que celui réservé au gestionnaire d'accès (gestionnaire local) lui-même ;

e) chaque utilisateur qui est désigné par une entreprise en tant que gestionnaire d'accès (gestionnaire local) ou désigné par le gestionnaire d'accès (gestionnaire local) d'une entreprise et qui dispose d'un nom d'utilisateur, d'un mot de passe, d'une clé privée et d'un certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale, a par ailleurs accès aux

applications reprises dans le tableau de l' « ANNEXE 2 – Applications via le site-portail de l'autorité fédérale », telles qu'elles sont indiquées pour lui.

f) 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 », telles qu'elles sont indiquées pour eux;

b) chaque utilisateur habilité a, selon sa qualité, accès aux applications reprises dans le tableau de l' « ANNEXE 3 - applications via le site-portail eSanté », telles qu'elles sont indiquées pour lui;

c) chaque utilisateur habilité a accès aux applications reprises dans le tableau de l' « ANNEXE 3 - applications via le site-portail eSanté », telles qu'elles sont indiquées pour lui;

d) 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.

4. Par le biais du système de transmission de fichiers en (S)FTP ou d'autres canaux acceptés, chaque utilisateur qui est désigné par une entreprise en tant que gestionnaire d'accès (gestionnaire local) ou par un gestionnaire d'accès (gestionnaire local) et qui dispose d'un nom d'utilisateur, d'un mot de passe, d'une clé privée et d'un certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site- portail de la sécurité sociale, dont le certificat de signature activé de la carte d'identité électronique, peut effectuer des « Déclarations Dimona », des « Déclarations DmfA – Déclaration multifonctionnelle », des « Déclarations DmfA pour les administrations provinciales et locales », des « Modifications d'une déclaration à l'ONSS » des "Modifications d'une déclaration- DmfAPPL » et des « DRS - Déclarations de risques sociaux ».

Le contenu des services et l'accès à ces services peuvent être modifiés à tout moment.

Des modalités d'utilisation spécifiques des services offerts peuvent être spécifiées en annexe du présent règlement d'utilisation.

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 – Usage du nom d'utilisateur et du mot de passe

Un utilisateur désigné par une entreprise en tant que gestionnaire d'accès principal peut recevoir un nom d'utilisateur et un mot de passe dans des messages séparés, envoyés par Eranova, le Centre de Contact des institutions publiques de sécurité sociale. Un utilisateur qui n'a pas été désigné comme gestionnaire d'accès principal par une entreprise se voit attribuer son nom d'utilisateur et son mot de passe par le gestionnaire d'accès (gestionnaire local) d'une entreprise.

Le nom d'utilisateur et le mot de passe sont strictement personnels et intransmissibles.

Chaque utilisateur est tenu de modifier le plus rapidement possible après réception ou du moins au moment de la première utilisation, le mot de passe qu'il s'est vu attribuer par le Centre de Contact des institutions publiques de sécurité sociale ou par un gestionnaire d'accès (gestionnaire local). Ensuite, chaque utilisateur devra modifier régulièrement son mot de passe.

Un mot de passe sécurisé est composé de 15 signes et contient des caractères et des symboles alphanumériques placés dans un ordre difficile à déceler. Chaque utilisateur doit veiller à ce que le mot de passe choisi réponde à ces conditions. La responsabilité de chaque utilisateur est engagée lorsqu'un mot de passe qui n'a pas été composé en respectant ces règles, est décelé et/ou utilisé de manière illicite.

Il appartient à chaque utilisateur de faire un usage judicieux de ses noms d'utilisateur et mot de passe et d'assurer le secret en ce domaine. Chaque utilisateur assume la responsabilité de tout usage approprié ou non de ses nom d'utilisateur et mot de passe, en ce compris l'usage par des tiers.

Lorsqu'un utilisateur est au courant de la perte de son nom d'utilisateur et/ou mot de passe ou d'une quelconque utilisation inappropriée de son nom d'utilisateur et/ou mot de passe par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée, il doit prendre immédiatement toutes les mesures nécessaires.

Tout utilisateur qui est désigné par une entreprise en tant que gestionnaire d'accès principal doit, entre autres, signaler immédiatement cette perte ou cette utilisation inappropriée au Centre de Contact des institutions publiques de sécurité sociale, Eranova (02/511.51.51 ou par le site-portail de la sécurité sociale (www.securitesociale.be)). Dans les plus brefs délais de la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour modifier le nom d'utilisateur et le mot de passe de l'utilisateur.

Tout utilisateur qui n'est pas désigné par une entreprise comme gestionnaire d'accès principal est tenu, entre autres, de signaler immédiatement cette perte ou cet usage inapproprié au gestionnaire d'accès principal ou au gestionnaire d'accès (gestionnaire local) dont il a reçu le nom d'utilisateur ou le mot de passe. Dès réception de ce message, ce dernier doit, dans les limites du raisonnable, mettre tout en œuvre pour rendre inactif et/ou modifier le nom d'utilisateur et le mot de passe de l'utilisateur.

Chaque utilisateur continue à assumer la responsabilité de tout dommage (direct ou indirect) causé par l'utilisation (appropriée ou non) de son nom d'utilisateur et/ou de son mot de passe avant l'inactivation du nom d'utilisateur et du mot de passe.

En cas de blocage du nom d'utilisateur et/ou du mot de passe, l'utilisateur désigné par une entreprise en tant que gestionnaire d'accès (gestionnaire local) doit demander un nouveau nom d'utilisateur et un nouveau mot de passe auprès de Eranova, Centre de Contact des institutions publiques de sécurité sociale. Ensuite, un nouveau nom d'utilisateur et un nouveau mot de passe sont fournis.

Article 5 bis – 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, 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 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 prescriptions 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 du certificat

L'accès de l'utilisateur à certains services suppose soit l'utilisation d'une carte d'identité électronique, soit, outre l'utilisation d'un nom d'utilisateur et d'un mot de passe, l'usage d'une clé privée et d'un certificat qualifié au sens de l'article 2, 4°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale.

Un même certificat peut être utilisé pour l'authentification et pour l'apposition d'une signature électronique visée à l'article 1322, alinéa 2, du Code civil. Cependant, 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 des données afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité de ces données. En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature 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 les données afférentes à la création de signature correspondantes 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. L'utilisateur doit conserver la clé privée et le certificat sur un support sécurisé, de préférence sur une carte à puce qui ne permet pas d'exporter la clé privée.

Le système d'information est en mesure de valider des certificats et des types délivrés par les autorités de certification qui figurent dans la liste publiée sur le site-portail de la sécurité sociale (www.securitesociale.be). Les certificats délivrés par d'autres autorités de certification ne peuvent être acceptés que dans la mesure où les adaptations techniques nécessaires à la validation de ces certificats auront été apportées au système d'information. Un utilisateur souhaitant à tout prix utiliser un certificat qualifié au sens de l'article 2, 4°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, qui a été délivré par une autorité de certification différente de celles mentionnées dans le site-portail de la sécurité sociale, peut en faire la demande en faisant usage de son nom d'utilisateur et son mot de passe par le biais du formulaire réservé à cet effet sur le site-portail de la sécurité sociale. Dans les limites du raisonnable et pour autant que l'autorité de certification en question apporte sa nécessaire collaboration, tout sera mis en œuvre pour que le système d'information valide également les certificats de l'autorité de certification susvisée. Une fois ces opérations réalisées, les certificats de l'autorité de certification en question pourront être utilisés.

Article 8 – Utilisation des signatures électroniques et justification (les utilisateurs titulaires d'un certificat).

Les messages envoyés via le système d'information par l'utilisateur qui dispose soit d'un certificat qualifié au sens de l'article 2, 4° de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ou de tout autre type de certificat qui figure sur la liste des certificats acceptés publiée sur le site-portail de la sécurité sociale, soit d'une 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 par 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 la clé privée et du certificat qui lui a été attribué, 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.

Article 10bis – Licences libres

Lorsque le système d'information et les services utilisent ou mettent à disposition un logiciel libre, la licence attachée à ce logiciel s'applique à l'utilisateur.

Outre les règles contenues dans la licence du logiciel libre concerné, les dispositions indépendantes et complémentaires suivantes, réglant la responsabilité des gestionnaires, administrateurs, collaborateurs et agents du système d'information (ci-après appelés « le système d'information ») et la garantie offerte par eux, s'appliquent à l'utilisateur.

Lorsque le système d'information adapte un logiciel libre, il met tout en œuvre pour en permettre une correcte utilisation par l'utilisateur, sans toutefois assumer aucune obligation de résultat à cet égard.

De son côté, l'utilisateur s'engage à utiliser le logiciel ainsi mis à sa disposition de la manière la plus adéquate et correcte qui soit et, le cas échéant, à transmettre au système d'information toute information utile permettant de tenter de résoudre les problèmes d'utilisation du logiciel.

Etant donné l'utilisation du logiciel concerné est libre, le système d'information ne pourra en aucun cas, sauf mention écrite, être tenu pour responsable de tout dommage direct, indirect, secondaire ou accessoire, matériel ou moral, subis par l'utilisateur ou par des tiers, découlant de l'utilisation du logiciel ou de l'impossibilité d'utiliser celui-ci.

Article 11 – Mesures transitoires

Pour l'heure, le certificat de signature de la carte d'identité électronique ne peut être utilisé que via le système de transmission de fichiers en (S)FTP, à l'aide de MQSeries ou d'autres canaux acceptés, et ne permet pas l'accès aux services dispensés sur le site-portail de la sécurité sociale

et sur le site-portail de l'autorité fédérale et leur utilisation, sauf pour ce qui concerne l'utilisation de l'application "Formulaire électronique de demande d'accès".

Article 12 – Moyens d'authentification et niveaux d'assurance

Les moyens d'authentification sont utilisés pour établir de manière fiable l'identité d'un utilisateur et sont essentiels à la sécurité numérique et au contrôle d'accès.
Le Federal Authentication Service (FAS) de SPF BOSA propose divers moyens pour ce faire, qui sont utilisés par exemple par la BCSS et la plateforme eHealth pour donner aux citoyens et aux professionnels un accès sécurisé à des applications sensibles.

Le niveau de confiance (ou niveau d'assurance) d'une authentification signifie à quel point il est certain que quelqu'un est vraiment celui qu'il prétend être – on parle de faible, substantiel ou élevé selon les réglementations européennes. FAS spécifie également ce niveau avec un numéro (le niveau d'authentification FAS) pour une plus grande précision.
Le SPF BOSA publie un aperçu des ressources disponibles:

Niveaux d'assurance	FAS Niveaux d'autentification	Moyens d'authentification
Élevé	500	eID
		eIDAS4 Elevé
	490	MyGov.be Elevé (avec PIN)
	450	Itsme Elevé (avec PIN)
Substantiel	400	eIDAS Substantiel
		Itsme Substanciel (avec empreinte digitale)
		MyGov.be Substanciel (avec empreinte digitale)
		TOTP (par Authenticator App)
		TOTP (par mail)
		TOTP (par SMS)
Faible	200	Username / Password

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

<table>
<tr><td></td><td>UID/PWD
+ futur

(faible)</td><td>eID
ITSME
X509 cert.
TOTP
MyGov.be
eIDAS
+ futur

(substantiel & élevé)</td></tr>
<tr><td></td><td>Niveau suffisant
OUI/NON</td><td>Niveau suffisant
OUI/NON</td></tr>
<tr><td colspan="3">Applications accessibles pour chaque utilisateur comme décrit à l’article 3.1.a</td></tr>
<tr><td>Dimona (non sécurisée)</td><td colspan="2" rowspan="7">Pour ces applications, aucune clé numérique n’est requise</td></tr>
<tr><td>Déclarations de travaux</td></tr>
<tr><td>Formulaire électronique de demande d’accès</td></tr>
<tr><td>Consultation publique du répertoire des employeurs</td></tr>
<tr><td>Identification des employeurs (WIDE) - non sécurisé</td></tr>
<tr><td>Obligation de retenue</td></tr>
<tr><td>Plan de paiement amiable</td></tr>
<tr><td colspan="3">Applications accessibles pour les curateurs comme décrit à l’article 3.1.b</td></tr>
<tr><td>eCUR</td><td rowspan="2">Oui</td><td rowspan="2">Oui</td></tr>
<tr><td>Identification des employeurs (WIDE)</td></tr>
<tr><td colspan="3">Applications accessibles pour les gestionnaires d’accès (gestionnaires locaux) et les utilisateurs désignés par eux comme décrit aux articles 3.1.c et 3.1.d</td></tr>
<tr><td>« Consultation de la e-Box »,</td><td rowspan="10">Oui</td><td rowspan="10">Oui</td></tr>
<tr><td>« Dimona (sécurisé) »,</td></tr>
<tr><td>« DmfA - déclaration multifonctionnelle »,</td></tr>
<tr><td>« DmfA pour les administrations provinciales et locales »,</td></tr>
<tr><td>« DRS - Déclaration risques sociaux (introduire et modifier) »,</td></tr>
<tr><td>« Consultation sécurisée du répertoire des employeurs »,</td></tr>
<tr><td>« Consultation fichier de vacances »,</td></tr>
<tr><td>“Limosa - Meldingsplicht”,</td></tr>
<tr><td>« Gestion des accès pour les entreprises et organisations,</td></tr>
</table>

	UID/PWD + futur (faible)	eID ITSME X509 cert. TOTP MyGov.be eIDAS + futur (substantiel & élevé)
	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON
Applications accessibles pour les gestionnaires d'accès (gestionnaires locaux) et les utilisateurs désignés par eux comme décrit dans les articles 3.1.c et l'article 3.1.d		
"Ecaro",	Oui	Oui
« Trillium »,		
« Identification des employeurs (WIDE) »,		
« Capelo - Compléments au Dossier de carrière »,		
" Capelo - Données Historiques",		
« Student@Work »,		
« DestHa - Gestion règles d'expédition du destinataire habilité »,		
« Consultation factures employeurs »,		
« Checkinatwork »,		
« Horeca@work »,		
« Publiato »,		
« Déclaration de travaux - FRONTEND »,		
« Obligation de retenue »,		
« FollowIt »		
« Gestion et historique des mandats de sécurité sociale (Mahis) »	Non	Oui
"DB2P",		
« Mandataires publics »,		
« Travailler à l'étranger »		
« modification d'une déclaration à l'ONSS (DMFA) »		
« modification d'une déclaration DmfAPPL »		
S'enregistrer sur le Portail (sécurisé)		
Travailler à l'étranger - Indépendants		
Green@Work		
Rina		
BelgianIDpro		
Dispense cotisations sociales travailleurs indépendants		
ContactData		
CareerPro Documents		
« Chômage temporaire et livre de validation »,		
Dossier interruption de carrière et crédit-temps		
Travail associatif	Non	Oui
Working in the Arts – Indemnité des arts en amateurs	Non	Oui
Check In and Out at Work	Non	Oui
Chaman : gestion des canaux techniques	Non	Oui
CareerPro Federal Learning Account	Non	Oui
Flexi at work	Non	Oui
Mandats Citoyen	Non	Oui
Consultation des données du citoyen	Non	Oui
Mesures de promotion de l'employabilité	Oui	Oui
Surveillance de la santé des travailleuses enceintes	Non	Oui

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

	UID/PWD + futur (faible)	eID ITSME X509 cert. TOTP MyGov.be eIDAS + futur (substantiel & élevé)
	Niveau suffisant OUI/NON	Niveau Suffisant OUI/NON
Consultation d'informations auprès des entreprises	Pour ces applications, aucune clé numérique n'est requise	
Applications accessibles pour les gestionnaires d'accès (gestionnaires locaux) et les utilisateurs désignés par eux comme décrit dans les articles 3.2.b et 3.2.d		
« Consultation des données de mon entreprise »	Oui	Oui
« Enquête de mobilité domicile - travail »		
« Vigilis (e-guichet) »		
« e-Notification »		
« La Déclaration unique pour les starters (DEUS) »		
Applications accessibles pour les gestionnaires d'accès (gestionnaires locaux) et les utilisateurs désignés par eux comme décrit dans les articles 3.2.c et 3.2.d		
"Tax-on-web" (TOW)	Oui	Oui
« Consultation de la déclaration Tax-on-web »		
Applications accessibles pour les gestionnaires d'accès (gestionnaires locaux) et les utilisateurs désignés par eux comme décrit à l'article 3.2.e		
"Belcotax-on-web"	Non	Oui
"PLDA – Paperless Douane en Accijnzen".		

ANNEXE 3 - Applications via le site-portail eSanté

<table>
<tr><td></td><td>UID/PWD
+ futur

(faible)</td><td>eID
ITSME
X509 cert.
TOTP
MyGov.be
eIDAS
+ futur

(substantiel & élevé)</td></tr>
<tr><td></td><td>Niveau suffisant OUI/NON</td><td>Niveau suffisant OUI/NON</td></tr>
<tr><td colspan="3">Applications accessibles pour chaque utilisateur comme décrit à l’article 3.3.a</td></tr>
<tr><td>« Source authentique dispositifs médicaux implantables »</td><td colspan="2" rowspan="3">Pour ces applications, aucune clé numérique n’est requise</td></tr>
<tr><td>Pharma formulary</td></tr>
<tr><td>« Healthdata.be Data Reporting »</td></tr>
<tr><td colspan="3">Applications accessibles pour chaque utilisateur habilité en fonction de sa qualité comme décrit à l’article 3.3.b</td></tr>
<tr><td>« BHOD - Honoraires de disponibilité »</td><td rowspan="2">Oui</td><td rowspan="2">Oui</td></tr>
<tr><td>« CEBAM Digital Library for Health / DCLH / EBMPRACTICENET »,</td></tr>
<tr><td>« E-loket zorg en gezondheid »,</td><td rowspan="8">Non</td><td rowspan="8">Oui</td></tr>
<tr><td>« WebWachtMailer »;</td></tr>
<tr><td>« eHealth Web Application for File Exchange for Batch applications (WebFX) »;</td></tr>
<tr><td>« eTCT - Feed-back aux hôpitaux sur leurs prestations de soins et sur leur coût »</td></tr>
<tr><td>UPPAD</td></tr>
<tr><td>« BINC (Begeleiding in Cijfers) - Système d’enregistrement en ligne dédié aux établissements privés du secteur de l’aide spéciale à la jeunesse »,</td></tr>
<tr><td>« Platform Welzijn en Gezondheid » ;</td></tr>
<tr><td>« Interface for communication on experiments between sponsors, ethics committees and the competent authority (ICE-SEC) »:</td></tr>
<tr><td colspan="3">Applications accessibles pour chaque utilisateur habilité comme décrit à l’article 3.3.c</td></tr>
<tr><td>« Système électronique d’échange de données pour la Vlaams Agentschap Zorg & Gezondheid (VESTA) »,</td><td rowspan="9">Non</td><td rowspan="9">Oui</td></tr>
<tr><td>« Enregistrement du cancer »</td></tr>
<tr><td>« Cellule technique via le web (eTCT) »,</td></tr>
<tr><td>« Notification électronique de naissance (eBirth) »,</td></tr>
<tr><td>« Consultation assurabilité d’une personne »,</td></tr>
<tr><td>« Envoyer des factures tiers payant »</td></tr>
<tr><td>« eBox Update Info »</td></tr>
<tr><td>« Project on Cancer of the Rectum, application en ligne pour l’enregistrement du cancer du rectum (PROCARE DATA ENTRY) »</td></tr>
<tr><td>« Medic-e intern - Alimentation et consultation électroniques des évaluations de personnes handicapées »,</td></tr>
<tr><td>« Tool for Administrative Reimbursment Drugs Information Sharing » (TARDIS),</td><td rowspan="2">Non</td><td rowspan="2">Oui</td></tr>
<tr><td>« ODEA »,</td></tr>
</table>

	UID/PWD + futur (faible)	eID ITSME X509 cert. TOTP MyGov.be eIDAS + futur (substantiel & élevé)
	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON
Applications accessibles pour chaque utilisateur habilité comme décrit à l'article 3.3.c		
« ORTHOpedic Prosthesis Identification Data - Electronic Registry - ORTHOpride® »,	Non	Oui
« Project on cancer of the rectum - Central Image Repository (PROCARE RX) »,		
« Qermid(c)Pacemakers-Quality Electronic Registration of Medical Implant Devices »,		
« SMUREG »		
« Flux Médico-Administratifs - Infirmier à domicile (MEDADM-INF) »,		
« ZNA - Zorgportaal – Sarai »,		
« Enregistrement des projets thérapeutiques (TherPro – PatientRegistration) »,		
« BHOD - Honoraires de disponibilité »,		
« QermidDefibrilateur-Quality Electronic Registration of Medical Implant Devices »,		
« eHealth box »,		
« QermidEndoprothèses-Quality Electronic Registration of Medical Implant Devices » »,		
« QermidPacemakers-Quality Electronic Registration of Medical Implant Devices »,		
« QermidTuteurs Coronaires-Quality Electronic Registration of Medical Implant Devices »,		
« Module d'enregistrement de la tumorothèque virtuelle belge »,		
« Catalogue de la Tumorothèque Virtuelle Belge »,		
« CIVARS – Chapter IV Agreement Requesting System »,		
« Web Application Metahub »,		
« consultation de la carte médicale »,		
« TDI - Module d'enregistrement "Treatment Demand Indicator »,		
« eShop - Commande en ligne des attestations de soins (Medattest) »,		
« BNMDR - Belgian NeuroMuscular Disease Registry", "eHealthConsent »,		
« Moduledatabank Jeugdhulp Vlaanderen »,		
« Source authentique médicaments »,		
« Insisto - système informatique Passerelle intersectorielle »,		
« Consultation du droit DMG »		
PCR Prescription validation		
"DOMINO",		

	UID/PWD + futur (faible)	eID ITSME X509 cert. TOTP MyGov.be eIDAS + futur (substantiel & élevé)
	Niveau suffisant OUI/NON	Niveau suffisant OUI/NON
Applications accessibles pour chaque utilisateur habilité comme décrit à l'article 3.3.c		
« Registre central de traçabilité », « eTarif », « eHealth box », « Statistiek Jongerenwelzijn », « GKB2.0 - fichier de clients commun », « PARIS (Prescription & Autorisation Requesting Information System) », « BelRAI », « eHealth API portal ». eHealthCreaBis BelRAI Vlaanderen Corona Vaccination - Application de déclaration des patients atteints d'une maladie rare/complexe Corona Test prescription & Consultation MyINAMI Heracles MediPrima	Non	Oui
Software Register - cadastre officiel et partagé des logiciels de santé	Non	Oui

Annexe 4 - Utilisation de la source authentique des médicaments par les développeurs de logiciels

1. Introduction

La Source authentique des médicaments est mise à disposition par la Plate-forme eHealth via son site portail.

La Source authentique des médicaments contient des données en provenance de l'Agence fédérale des médicaments et des produits de santé (AFMPS) et de l'Institut national d'assurance maladie-invalidité (INAMI).

2. Mise à la disposition des développeurs de logiciels

Les développeurs de logiciels qui développent des logiciels agréés ou enregistrés pour les prestataires de soins peuvent télécharger la Source authentique des médicaments dans son intégralité à partir du site portail de la Plate-forme eHealth.

Les modalités de la mise à disposition des mises à jour éventuelles seront publiées sur le site portail de la plate-forme eHealth.

3. Utilisation de la Source authentique des médicaments

Les développeurs de logiciels peuvent uniquement utiliser la Source authentique des médicaments en vue de son intégration dans leurs logiciels agréés ou enregistrés pour les prestataires de soins.

A l'exception des frais éventuels pour l'intégration technique de la Source authentique des médicaments dans les logiciels, il est interdit aux développeurs de logiciels de demander une rémunération pour la mise à disposition du contenu de la Source authentique des médicaments au profit des utilisateurs des logiciels.

Le contenu de la Source authentique des médicaments ne peut être utilisé d'aucune façon à des fins publicitaires ou commerciales par les développeurs de logiciels ou des tiers.

Les droits intellectuels ou droits d'auteur liés aux données présentes dans la Source authentique des médicaments appartiennent exclusivement aux parties ayant fourni les données à la Source authentique des médicaments, à savoir l'AFMPS et l'INAMI.

Il est interdit aux développeurs de logiciels de modifier les données contenues dans la Source authentique des médicaments en modifiant ou supprimant entièrement ou partiellement le contenu.

Les développeurs de logiciels sont autorisés à enrichir la Source authentique des médicaments avec d'autres données, mais uniquement sous leur propre responsabilité et en le mentionnant explicitement aux utilisateurs.

4. Responsabilités

L'AFMPS, l'INAMI, la Plate-forme eHealth et toute autre partie concernée par la constitution et la mise à disposition de la Source authentique des médicaments mettent tout en œuvre pour une constitution et mise à disposition correctes de la Source authentique des médicaments, sans toutefois se soumettre à une obligation de résultat à cet égard.

L'AFMPS, l'INAMI, la Plate-forme eHealth et toute autre partie concernée par la constitution et la mise à disposition de la Source authentique des médicaments sont déchargés de toute responsabilité en ce qui concerne l'utilisation concrète des informations disponibles dans la Source authentique des médicaments. Ils ne peuvent en aucun cas être tenus responsables des dommages quelconques, directs ou indirects, secondaires ou complémentaires, matériels ou immatériels, causés auprès de l'utilisateur ou de tiers et résultant de l'utilisation de la Source authentique des médicaments ou de l'impossibilité de l'utiliser.

5. Infractions et dédommagement

En cas d'infraction aux conditions d'utilisation, le développeur de logiciels sera redevable d'un dédommagement de € 50.000 à l'AFMPS, à l'INAMI et à la Plate-forme eHealth à titre collectif.

Dans l'hypothèse où la Plate-forme eHealth, l'AFMPS ou l'INAMI constatent une infraction à une ou plusieurs conditions d'utilisation par un développeur de logiciels, ce dernier en sera informé. Le développeur de logiciels est ensuite tenu de mettre immédiatement et définitivement fin à l'utilisation de la Source authentique des médicaments sous peine d'une indemnisation supplémentaire de € 5.000 pour les parties précitées par jour de retard.