KONINKRIJK BELGIË

FEDERALE OVERHEIDSDIENST INFORMATIE- EN COMMUNICATIETECHNOLOGIE

Voorontwerp van wet inzake elektronische identificatie

ROYAUME DE BELGIQUE

SERVICE PUBLIC FÉDÉRAL TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION

Avant-projet de loi relative à l'identification électronique

Hoofdstuk 1. Algemene bepaling

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Chapitre 1er. Disposition générale

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Hoofdstuk 2. Definities en toepassingsgebied

Afdeling 1. Definities

Artikel 2. Deze wet voert enerzijds hoofdstuk II (elektronische identificatie) van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG uit, en legt anderzijds bepaalde regels vast in verband met het juridisch kader voor elektronische identificatiemiddelen voor overheidstoepassingen in België.

Chapitre 2. Définitions et champ d'application

Section 1ère. Définitions

Article 2. La présente loi exécute d'une part le chapitre II (identification électronique) du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, et fixe d'autre part certaines règles liées au cadre juridique des moyens d'identification électronique sur des applications publiques en Belgique.

Artikel 3. § 1. Voor de toepassing van deze wet en de uitvoeringsbesluiten wordt verstaan onder:

1° verordening 910/2014: de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

2° uitvoeringsverordening (EU) 2015/1501: de uitvoeringsverordening (EU) 2015/1501 van de Commissie van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van verordening 910/2014

Article 3. § 1er. Pour l'application de la présente loi et des arrêtés d'exécution, on entend par :

1° règlement 910/2014 : le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

2° règlement d'exécution (UE) 2015/1501 : le règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement 910/2014 ;

3° uitvoeringsverordening (EU) 2015/1502: de uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 van de Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3 van verordening 910/2014;

3° règlement d'exécution (UE) 2015/1502 : le règlement d'exécution (UE) 2015/1502 de la Commission européenne du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement 910/2014 ;

4° toezichthoudend orgaan: het orgaan bestaande uit experten van de Federale Overheidsdienst Binnenlandse Zaken, van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie en van de Federale Overheidsdienst Informatie- en Communicatietechnologie, dat belast is met het toezicht op de door de overheid aangemelde stelsels voor elektronische identificatie;

4° organe de contrôle : l'organe se composant d'experts du Service public fédéral Intérieur, du Service public fédéral Économie, PME, Classes moyennes et Énergie et du Service public fédéral Technologie de l'Information et de la Communication, qui est chargé du contrôle des schémas d'identification électronique notifiés par l'Administration ;

§ 2. De begrippen die in hoofdstuk 3 van deze wet voorkomen en die niet in paragraaf 1 van dit artikel worden gedefinieerd, worden begrepen in de zin van de definities van artikel 3 van verordening 910/2014.

§ 2. Les concepts mentionnés dans le chapitre 3 de la présente loi et qui ne sont pas définis au paragraphe 1er du présent article, sont compris au sens des définitions de l'article 3 du règlement 910/2014.

Afdeling 2. Toepassingsgebied

Section 2. Champ d'application

Artikel 4. § 1. Hoofdstuk 3 van deze wet is van toepassing op Belgische stelsels voor elektronisch identificatie die aangemeld werden bij de Commissie overeenkomstig artikel 9 van verordening 910/2014, de verantwoordelijken daarvan en op partijen die een elektronisch identificatiemiddel uitgeven of die een authenticatieprocedure uitvoeren in het kader van een aangemeld stelsel voor elektronische identificatie.

Article 4. § 1er. Le chapitre 3 de la présente loi s'applique aux schémas d'identification électronique belges qui ont été notifiés à la Commission conformément à l'article 9 du règlement 910/2014 ainsi qu'aux leurs responsables et aux parties qui délivrent un moyen d'authentification électronique ou qui gèrent une procédure d'authentification dans le cadre d'un schéma d'identification électronique notifié.

§ 2. Hoofdstuk 4 van deze wet is van toepassing op diensten voor elektronische identificatie waarmee toegang kan worden verkregen tot Belgische digitale overheidstoepassingen.

§ 2. Le chapitre 4 de la présente loi s'applique aux services d'identification électronique permettant d'accéder à des applications publiques numériques belges.

Hoofdstuk 3. Grensoverschrijdende elektronische identificatie

Chapitre 3. Identification électronique transfrontalière

Afdeling 1. Wederzijdse erkenning

Section 1ère. Reconnaissance mutuelle

Artikel 5. § 1. Aan de vereiste van een Belgisch elektronisch identificatiemiddel om toegang te krijgen tot een onlinedienst

Article 5. § 1er. L'exigence d'un moyen d'identification électronique belge pour accéder à un service en ligne offert par une

aangeboden door een openbare instantie in België, is voldaan door om het even welk elektronisch identificatiemiddel uitgegeven in een andere lidstaat dat voldoet aan de voorwaarden van artikel 6 van verordening 910/2014.

§ 2. Om toegang te krijgen tot een onlinedienst aangeboden door een andere vertrouwende partij dan een openbare instantie, kan gebruik worden gemaakt van een door de Belgische overheid aangemeld stelsel voor elektronische identificatie wanneer voldaan is aan de voorwaarden gesteld door de Koning, bij in Ministerraad overlegd besluit.

Afdeling 2. Betrouwbaarheidsniveaus

Artikel 6. § 1. Elke Belgische openbare instantie bepaalt de betrouwbaarheidsniveaus vereist voor de toegang tot haar online diensten in overeenstemming met de niveaus vervat in artikel 8 van verordening 910/2014 en informeert hierover de federale overheidsdienst Informatie- en Communicatietechnologie.

§ 2. De federale overheidsdienst Informatie- en Communicatietechnologie bepaalt, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, de betrouwbaarheidsniveaus voor de bij de Commissie aan te melden elektronische identificatiemiddelen in overeenstemming met Uitvoeringsverordening (EU) 2015/1502, en zorgt voor aanmelding van één of meerdere Belgische stelsels voor elektronische identificatie overeenkomstig artikel 9 van verordening 910/2014.

Afdeling 3. Persoonsidentificatiegegevens en toegang tot het Rijksregister

Artikel 7. § 1.De federale overheidsdienst Informatie- en Communicatietechnologie geeft in overeenstemming met artikel 11 en

instance publique en Belgique, est respectée par tout moyen d'identification électronique délivré dans un autre État membre et répondant aux conditions de l'article 6 du règlement 910/2014.

§ 2. Pour accéder à un service en ligne offert par une autre partie utilisatrice qu'une instance publique, il est possible d'utiliser un schéma d'identification électronique notifié par les autorités belges lorsque les conditions posées par le Roi, par un arrêté délibéré en Conseil des Ministres, ont été respectées.

Section 2. Niveaux de garantie

Article 6. § 1er. Toute instance publique belge détermine les niveaux de garantie exigés pour accéder à ses services en ligne conformément aux niveaux mentionnés à l'article 8 du règlement 910/2014 et informe le service public fédéral Technologie de l'Information et de la Communication.

§ 2. Le service public fédéral Technologie de l'Information et de la Communication détermine, après consultation du Collège des présidents des services publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, les niveaux de garantie pour les moyens d'identification électronique à notifier à la Commission conformément au Règlement d'exécution (UE) 2015/1502, et se charge de la notification d'un ou de plusieurs schémas d'identification électronique belges conformément à l'article 9 du règlement 910/2014.

Section 3. Données d'identification personnelle et accès au Registre national

Article 7. § 1er. Le service public fédéral Technologie de l'Information et de la Communication transmet, conformément à

de bijlage van de uitvoeringsverordening (EU) 2015/1501, het minimale pakket persoonsidentificatiegegevens van de houder van een door België aangemeld elektronisch identificatiemiddel, die zich wenst te identificeren voor toegang tot een onlinedienst aangeboden in een andere lidstaat, door aan het knooppunt van die lidstaat.

§ 2. Voor de uitvoering van de verplichting vermeld in § 1, wordt de federale overheidsdienst Informatie- en Communicatietechnologie gemachtigd om de in §1 bedoelde gegevens op te halen in het Rijksregister.

§ 3. Om te voldoen aan een verplichting van de verordening 910/2014 of één van haar uitvoeringshandelingen die de uitwisseling van bijkomende optionele persoonsidentificatiegegevens mogelijk maakt, wordt de federale overheidsdienst Informatie- en Communicatietechnologie gemachtigd, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, om de overeenkomstige gegevens op te halen in het Rijksregister.

l'article 11 et à l'annexe du règlement d'exécution (UE) 2015/1501, l'ensemble minimal de données d'identification personnelle du titulaire d'un moyen d'identification électronique notifié par la Belgique, qui souhaite s'identifier pour accéder à un service en ligne offert dans un autre État membre, au nœud de cet État membre.

§ 2. Pour l'exécution de l'obligation mentionnée au § 1er, le service public fédéral Technologie de l'Information et de la Communication est autorisé à obtenir du Registre national les données visées au § 1er.

§ 3. Pour satisfaire à une obligation du règlement 910/2014 ou à l'un de ses actes d'exécution qui permet l'échange de données d'identification personnelle facultatives supplémentaires, le service public fédéral Technologie de l'Information et de la Communication est autorisé, après avis de la Commission de la protection de la vie privée, à obtenir du Registre national les données correspondantes.

Afdeling 4. Toezicht en controle

Artikel 8. § 1. Onverminderd de bepalingen van verordening 910/2014, wordt het toezichthoudend orgaan belast met het toezicht op de door de overheid aangemelde stelsels voor elektronische identificatie.

§ 2. Het toezichthoudend orgaan kan een beroep doen op de diensten van een of meer deskundigen om het te helpen in zijn toezichtsopdracht. De aangewezen deskundigen moeten financieel en organisationeel onafhankelijk zijn van de partijen die elektronische identificatiemiddelen uitgeven of die de authenticatieprocedure uitvoeren.

§ 3. Wanneer het toezichthoudend orgaan vaststelt dat een partij die een elektronisch identificatiemiddel uitgeeft of een partij die een authenticatieprocedure uitvoert zich niet houdt aan de eisen van verordening 910/2014 of van deze wet, stelt het hem in

Section 4. Surveillance et contrôle

Article 8. § 1er. Sans préjudice des dispositions du règlement 910/2014, l'organe de contrôle est chargé de la surveillance des schémas d'identification électronique notifiés par l'Administration.

§ 2. L'organe de contrôle peut faire appel aux services d'un ou de plusieurs experts pour l'aider dans sa mission de surveillance. Les experts désignés doivent, financièrement et sur le plan organisationnel, être indépendants des parties qui délivrent des moyens d'identification électronique ou qui gèrent la procédure d'authentification.

§ 3. Lorsque l'organe de contrôle constate qu'une partie délivrant un moyen d'identification électronique ou une partie gérant une procédure d'authentification ne respecte pas les exigences du règlement

gebreke en stelt het een redelijke termijn vast in functie van de aard en de ernst van de tekortkoming, tijdens welke de in gebreke blijvende partij alle nodige maatregelen dient te hebben getroffen om die tekortkoming te verhelpen.

§ 4. Indien na afloop van de in de vorige paragraaf vermelde termijn de nodige maatregelen niet werden getroffen, kan de minister bevoegd voor digitale agenda of zijn gemachtigde, na advies van het toezichthoudend orgaan, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut en zonder afbreuk te doen aan bijzondere regels van toepassing op elektronische identificatiemiddelen of stelsels voor elektronisch identificatie,

a) het betreffende stelsel voor elektronische identificatie of authenticatie opschorten of intrekken;
b) de partij die een elektronisch identificatiemiddel uitgeeft of die een authenticatieprocedure uitvoert te gelasten onmiddellijk vertrouwende partijen op de hoogte te brengen van de genomen maatregelen;
c) maatregelen ter verbetering van de dienstverlening opleggen ten aanzien van de in gebreke blijvende partij.

§ 5. Wanneer het toezichthoudend orgaan vaststelt dat de integriteit van een aangemeld stelsel voor elektronische identificatie of van delen daarvan geschonden is, zal de minister bevoegd voor digitale agenda of zijn gemachtigde, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, het volledig stelsel of de aangetaste delen daarvan intrekken of opschorten en de andere lidstaten en de Europese Commissie hiervan op de hoogte

910/2014 ou de la présente loi, il la met en demeure et fixe un délai raisonnable en fonction de la nature et la gravité du manquement, pendant lequel la partie défaillante doit prendre toutes les mesures nécessaires pour remédier à ce manquement.

§ 4. Si, à l'issue du délai mentionné au paragraphe précédent, les mesures nécessaires n'ont pas été prises, le ministre compétent pour l'agenda numérique ou son mandataire peut, sur conseil de l'organe de contrôle, après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, et sans porter atteinte aux règles particulières applicables aux moyens d'identification électronique ou aux schémas d'identification électronique,

a) suspendre ou révoquer le schéma d'identification ou d'authentification électronique concerné ;
b) sommer la partie qui délivre un moyen d'identification électronique ou qui gère une procédure d'authentification d'avertir immédiatement les parties utilisatrices des mesures prises ;
c) imposer à la partie défaillante des mesures en vue de l'amélioration de la prestation de services.

§ 5. Lorsque l'organe de contrôle constate que l'intégrité d'une partie ou de la totalité d'un schéma d'identification électronique notifié est violée, le ministre compétent pour l'agenda numérique ou son mandataire, après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, révoquera ou suspendra le schéma entier ou les parties touchées et en informera les autres États membres ainsi que la Commission européenne conformément à l'article 10 du règlement 910/2014.

stellen conform artikel 10 van de verordening 910/2014.

§ 6. De Koning kan, bij in Ministerraad overlegd besluit, de overige maatregelen bepalen die de minister, zijn gemachtigde en het toezichthoudend orgaan kunnen treffen wanneer de bepalingen van deze wet of van verordening 910/2014 niet gerespecteerd worden.

§ 7. Het toezichthoudend orgaan rapporteert jaarlijks over haar controle-activiteiten op een stelsel voor elektronische identificatie aan de autoriteiten verantwoordelijk voor die stelsels.

§ 6. Le Roi peut, par un arrêté délibéré en Conseil des Ministres, déterminer les autres mesures que le ministre, son mandataire et l'organe de contrôle peuvent prendre lorsque les dispositions de la présente loi ou du règlement 910/2014 ne sont pas respectées.

§ 7. L'organe de contrôle fait annuellement rapport sur ses activités de contrôle portant sur un schéma d'identification électronique aux autorités qui sont responsables de ces schémas.

Afdeling 5. Samenwerking en interoperabiliteit

Artikel 9. Overeenkomstig artikel 3 van het Uitvoeringsbesluit 2015/296 van 24 februari 2015 van de Commissie tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van verordening 910/2014, wordt de federale overheidsdienst Informatie- en Communicatietechnologie aangewezen als één loket.

Section 5. Collaboration et interopérabilité

Article 9. Conformément à l'article 3 de la Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) n ° 910/2014, le service public fédéral Technologie de l'Information et de la Communication est désigné comme guichet unique.

Artikel 10. De federale overheidsdienst Informatie- en Communicatietechnologie wordt aangewezen als exploitant van een knooppunt, als bedoeld in artikel 2 van Uitvoeringsverordening 2015/1501.

Article 10. Le service public fédéral Technologie de l'Information et de la Communication est désigné comme exploitant d'un nœud, tel que visé à l'article 2 du règlement d'exécution 2015/1501.

Hoofdstuk 4. Elektronische identificatie voor Belgische overheidstoepassingen

Afdeling 1. Authenticatiedienst

Artikel 11. §1. Onverminderd de verplichtingen verbonden aan de verordening 910/2014, wordt de federale overheidsdienst voor Informatie- en Communicatietechnologie belast met het aanbieden van elektronische aanmeldingsdiensten voor overheidstoepassingen, binnen de authenticatiedienst.

Chapitre 4. Identification électronique pour applications publiques belges

Section 1ère. Service d'authentification

Article 11. §1er. Sans préjudice des obligations liées au règlement 910/2014, le service public fédéral Technologie de l'Information et de la Communication est chargé d'offrir des services d'identification électronique pour des applications publiques au sein du service d'authentification.

§ 2. De federale overheidsdienst voor Informatie- en Communicatietechnologie zorgt voor de beschikbaarheid van de authenticatiedienst.

§ 3. Voor de uitvoering van haar opdracht van authenticatie heeft de federale overheidsdienst voor Informatie- en Communicatietechnologie het recht om het identificatienummer van de natuurlijke personen opgenomen in het Rijksregister te gebruiken.

§ 2. Le service public fédéral Technologie de l'Information et de la Communication veille à la disponibilité du service d'authentification.

§ 3. Pour l'exécution de sa mission d'authentification, le service public fédéral Technologie de l'Information et de la Communication a le droit d'utiliser le numéro d'identification des personnes physiques inscrites au Registre national.

Afdeling 2. Erkenning van elektronische aanmeldingsdiensten

Artikel 12. § 1. Andere partijen dan openbare instanties kunnen hun diensten voor elektronische identificatie, die door de federale overheidsdienst voor Informatie- en Communicatietechnologie, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, zijn erkend, aanbieden voor toegang tot overheidstoepassingen binnen de authenticatiedienst.

§ 2. De Koning bepaalt, bij in Ministerraad overlegd besluit, de procedure, de voorwaarden en de gevolgen van de erkenning van diensten voor elektronische identificatie voor toegang tot overheidstoepassingen, aangeboden door andere partijen dan openbare instanties, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

§ 3. De federale overheidsdienst voor Informatie- en Communicatietechnologie publiceert de procedure, de voorwaarden en de gevolgen van de erkenning, op de website van de authenticatiedienst.

Section 2. Agrément de services d'identification électronique

Article 12. § 1er. Des parties autres que des instances publiques peuvent offrir leurs services d'identification électronique, agréés par le service public fédéral Technologie de l'Information et de la Communication, après consultation du Collège des présidents des service publics fédéraux et des **services publics de programmation**, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des **organismes d'intérêt public fédéraux** , pour accéder à des applications publiques au sein du service d'authentification.

§ 2. Le Roi détermine, par un arrêté délibéré en Conseil des Ministres, la procédure, les conditions et les conséquences relatives à l'agrément des services d'identification électronique pour accéder à des applications publiques, offerts par des parties autres que des instances publiques, après avis de la Commission de la protection de la vie privée.

§ 3. Le service public fédéral Technologie de l'Information et de la Communication publie sur le site web du service d'authentification la procédure, les conditions et les conséquences de l'agrément.

§ 4. Wanneer nuttig laat de federale overheidsdienst voor Informatie- en Communicatietechnologie zich bij de erkenning bijstaan door deskundigen.

§ 4. En cas de nécessité, le service public fédéral Technologie de l'Information et de la Communication se fait assister par des experts.

§ 5. De aanbieder van een erkende dienst voor elektronische identificatie wordt voor de toepassing van dit artikel beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en in die hoedanigheid gemachtigd om het rijksregisternummer te gebruiken uitsluitend voor aanbieding van de erkende dienst voor elektronische identificatie via de authenticatiedienst.

§ 5. Le fournisseur d'un service d'identification électronique agréé est, pour l'application du présent article, considéré comme un sous-traitant de l'autorité d'agrément au sens de l'article 5, alinéa 1, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, et est, en cette qualité, autorisé à utiliser le numéro de Registre national exclusivement pour offrir le service d'identification électronique agréé par le biais du service d'authentification.

§ 6 Onverminderd de bevoegdheden en actiemogelijkheden van andere overheden of controlediensten kan de federale overheidsdienst voor Informatie- en Communicatietechnologie de aanbieders van erkende diensten voor elektronische identificatie aan een controle onderwerpen bij klacht of vermoeden van niet-overeenstemming van de dienstverlening met de goedgekeurde erkenningsvoorwaarden.

§ 6 Sans préjudice des compétences et possibilités d'action d'autres autorités ou services de contrôle, le service public fédéral Technologie de l'Information et de la Communication peut soumettre à un contrôle les fournisseurs de services d'identification électronique agréés en cas de plainte ou de suspicion de non-conformité du service aux conditions d'agrément approuvées.

§ 7. Wanneer de federale overheidsdienst voor Informatie- en Communicatietechnologie vaststelt dat de dienstverlening niet overeenstemt met de goedgekeurde erkenningsvoorwaarden, legt hij de door de Koning, bij in Ministerraad overlegd besluit, bepaalde maatregelen op.

§ 7. Lorsque le service public fédéral Technologie de l'Information et de la Communication constate que la prestation de services n'est pas conforme aux conditions d'agrément approuvées, il impose les mesures déterminées par le Roi, par un arrêté délibéré en Conseil des Ministres.

§ 8. De Koning kan de vergoedingsregeling bepalen voor de aanbieders van erkende diensten voor elektronische identificatie.

§ 8. Le Roi peut déterminer le régime d'indemnités pour les fournisseurs de services d'identification électronique agréés.

Afdeling 3. Verplichtingen verbonden aan het elektronisch identificatiemiddel

Section 3. Obligations liées au moyen d'identification électronique

Artikel 13.

Article 13.

De houder van een elektronisch identificatiemiddel is ertoe gehouden alle nodige maatregelen te nemen om het elekronisch identificatiemiddel onder zijn exclusieve controle te houden, om diefstal, verlies of verspreiding van zijn elektronisch

Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour garder sous son contrôle exclusif le moyen d'identification électronique, pour prévenir le vol, la perte ou la divulgation de ce moyen d'identification

identificatiemiddel te voorkomen en om in geval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.

Wanneer het elektronische identificatiemiddel vervalt of ingetrokken wordt, mag de houder ervan na de vervaldatum of na intrekking het elektronisch identificatiemiddel niet meer wetens en willens gebruiken.

électronique et pour le révoquer immédiatement en cas de vol, de perte ou de divulgation.

Lorsque le moyen d'identification électronique vient à échéance ou est révoqué, son titulaire ne peut plus l'utiliser sciemment après la date d'échéance ou la révocation.

Hoofdstuk 5. Inwerkingtreding

Artikel 14. De Koning bepaalt de inwerkingtreding van hoofdstuk 3 van deze wet.

Gegeven te

Chapitre 5. Entrée en vigueur

Article 14. Le Roi détermine l'entrée en vigueur du chapitre 3 de la présente loi.

Donné à

VAN KONINGSWEGE:

PAR LE ROI:

De Vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post,

Le Vice-Premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste,

Alexander DE CROO

60899/4

KONINKRIJK BELGIË

FEDERALE OVERHEIDSDIENST INFORMATIE- EN COMMUNICATIETECHNOLOGIE

Voorontwerp van wet inzake elektronische identificatie

MEMORIE VAN TOELICHTING

A. ALGEMEEN

Het huidige voorontwerp kadert in het globale e-governmentbeleid van de regering. E-government of "elektronische administratie" omvat het uitbouwen van een informaticastructuur en het nemen van initiatieven om administraties, burgers en ondernemingen in staat te stellen de informatie- en communicatietechnologie te gebruiken voor digitale overheidstoepassingen. Bovendien past het voorontwerp in de digitale agenda van België omdat het op deze manier innovatie wil stimuleren en ondersteunen.

Een essentiële bouwsteen binnen e-government is de elektronische identificatie van burgers en ondernemingen.

Om deel te nemen aan e-government dienen de burger en de onderneming zich online te kunnen identificeren, authentiseren en aanmelden voor overheidstoepassingen. De burger en de onderneming hebben nood aan mogelijkheden om hun identiteit ook online makkelijk te kunnen bewijzen.

Dit voorontwerp van wet strekt er enerzijds toe verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna verordening 910/2014), voor wat betreft hoofdstuk II aangaande elektronische identificatie, toe te passen.

ROYAUME DE BELGIQUE

SERVICE PUBLIC FÉDÉRAL TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION

Avant-projet de loi relative à l'identification électronique

EXPOSÉ DES MOTIFS

CONSEIL D'ETAT
LEGISLATION
25 -01- 2017
RAAD VAN STATE
WETGEVING

A. GÉNÉRALITÉS

Le présent avant-projet s'inscrit dans la politique d'e-gouvernement globale du gouvernement. L'e-gouvernement ou « administration électronique » recouvre le développement d'une structure informatique et la prise d'initiatives afin de permettre aux administrations, aux citoyens et aux entreprises d'utiliser les technologies de l'information et de la communication dans le cadre d'applications publiques numériques. En outre, l'avant-projet s'inscrit dans le cadre de l'agenda numérique de la Belgique étant donné qu'il entend ainsi stimuler et soutenir l'innovation.

Un fondement essentiel de l'e-gouvernement est l'identification électronique des citoyens et des entreprises.

Pour participer à l'e-gouvernement, les citoyens et les entreprises doivent pouvoir s'identifier, s'authentifier et se connecter en ligne sur des applications publiques. Ils ont besoin de méthodes leur permettant de prouver facilement leur identité en ligne.

Le présent avant-projet de loi vise d'une part à appliquer le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (dénommé ci-après « règlement 910/2014 »), concernant le chapitre II portant sur l'identification électronique.

Anderzijds strekt dit voorontwerp van wet er toe de Belgische federale authenticatiedienst wettelijk te verankeren en mogelijkheden te voorzien om diensten voor elektronische identificatie te erkennen met het oog op het verkrijgen van toegang tot Belgische overheidstoepassingen.

Le présent avant-projet de loi vise d'autre part à ancrer légalement le service fédéral d'authentification belge et à prévoir des possibilités pour agréer des services d'identification électronique afin d'accéder à des applications publiques belges.

B. TOEPASSING HOOFDSTUK II VERORDENING 910/2014

Op 23 juli 2014 keurde de Europese wetgever verordening 910/2014 goed.

De hoofddoelstelling van die verordening is de invoering van een juridisch kader om het vertrouwen in elektronische transacties in de interne markt te vergroten. Deze verordening trekt de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen in maar neemt niettemin het merendeel van haar bepalingen over. Hiertoe worden enkele wijzigingen aangebracht en worden een aantal nieuwe bepalingen toegevoegd. Deze bepalingen hebben enerzijds betrekking op de wederzijdse erkenning op Europees niveau van de aangemelde stelsels voor elektronische identificatie en anderzijds op de vertrouwensdiensten voor elektronische handtekeningen, voor elektronische zegels, voor elektronische tijdstempels, voor elektronisch aangetekende bezorging alsook voor websiteauthenticatie.

De verordening 910/2014 telt zes hoofdstukken. De twee belangrijkste hoofdstukken zijn het tweede hoofdstuk over de "elektronische identificatie" en het derde hoofdstuk over de "vertrouwensdiensten", omdat ze substantiële nieuwigheden op die beide gebieden bevatten. De andere vier hoofdstukken (die respectievelijk betrekking hebben op de algemene bepalingen, de elektronische documenten, de gedelegeerde handelingen, de uitvoeringshandelingen en de slotbepalingen) bevatten "bijkomende" bepalingen, hoofdzakelijk met het oog op de werking van de twee voornoemde hoofdstukken.

B. APPLICATION DU CHAPITRE II DU RÈGLEMENT 910/2014

Le 23 juillet 2014, le législateur européen a approuvé le règlement 910/2014.

L'objectif principal de ce règlement est d'instaurer un cadre juridique afin d'accroître la confiance dans les transactions électroniques du marché intérieur. Ce règlement abroge la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques mais reprend néanmoins la majorité de ses dispositions. À cette fin, quelques modifications sont apportées et une série de nouvelles dispositions sont ajoutées. Ces dispositions concernent d'une part la reconnaissance mutuelle au niveau européen des schémas d'identification électronique notifiés et d'autre part les services de confiance pour les signatures électroniques, pour les cachets électroniques, pour l'horodatage électronique, pour l'envoi recommandé électronique ainsi que pour authentification du site internet.

Le règlement 910/2014 comporte six chapitres. Le deuxième chapitre sur l'« identification électronique » et le troisième chapitre sur les « services de confiance » constituent les deux chapitres principaux, étant donné qu'ils comprennent des nouveautés substantielles dans ces deux domaines. Les quatre autres chapitres (qui concernent respectivement les dispositions générales, les documents électroniques, les délégations de pouvoir, les dispositions d'exécution et les dispositions finales) comprennent des dispositions « complémentaires », principalement en vue du fonctionnement des deux chapitres précités.

Hoofdstuk II van verordening 910/2014 over de "elektronische identificatie" is van directe toepassing in Belgisch recht maar een aantal wetswijzigingen op Belgisch niveau, zoals hierna in de artikelsgewijze commentaar verder toegelicht, dragen ertoe bij de door de overheid aangemelde stelsels voor elektronische identificatie, en het beheer daarvan, in lijn te brengen met de verplichtingen van verordening 910/2014.
Hoewel het merendeel van de bepalingen van hoofdstuk II van verordening 910/2014 reeds in werking zijn getreden, treedt de verplichting voor lidstaten tot wederzijdse erkenning van elektronische identificatiemiddelen maar in werking op 29 september 2018. Voor die datum kunnen lidstaten niettemin vrijwillig beslissen om bij de Commissie aangemelde stelsels te aanvaarden.

In deze context strekt dit voorontwerp van wet ertoe hoofdstuk II van verordening 910/2014 ten uitvoer te brengen en aan te vullen. Daartoe wordt een wet betreffende elektronische identificatie aangenomen waarin wordt voorzien in een principe van wederzijdse erkenning voor door andere Europese lidstaten aangemelde elektronische identificatiemiddelen, een precisering van de betrouwbaarheidsniveaus, een toezichts- en controlemechanisme en bepalingen omtrent samenwerking en interoperabiliteit.

C. ELEKTRONISCHE IDENTIFICATIE VOOR BELGISCHE OVERHEIDSTOEPASSINGEN

Het tweede gedeelte van het voorontwerp heeft geen rechtstreekse link met de toepassing van verordening 910/2014, maar beoogt de invoering van een juridisch kader voor elektronische identificatie in de context van Belgische overheidstoepassingen.

Enerzijds betreft het de werking van de federale authenticatiedienst die identiteits- en toegangsbeheer doet voor Belgische overheidstoepassingen. Anderzijds voorziet het in de mogelijkheid om mobiele en niet mobiele elektronische identificatiemiddelen te erkennen die gebruikt kunnen worden om toegang te krijgen tot Belgische overheidstoepassingen. Daartoe wordt

Le chapitre II du règlement 910/2014 consacré à l'« identification électronique » s'applique directement en droit belge mais une série de modifications législatives au niveau belge, comme expliqué plus en détail ci-après dans le commentaire des articles, contribue à ce que les schémas d'identification électronique notifiés par l'administration, et leur gestion, répondent aux obligations du règlement 910/2014.
Bien que la majorité des dispositions du chapitre II du règlement 910/2014 soient déjà entrées en vigueur, l'obligation pour les États membres de reconnaissance mutuelle des moyens d'identification électronique n'entrera en vigueur que le 29 septembre 2018. Avant cette date, les États membres peuvent néanmoins volontairement décider d'accepter les schémas notifiés à la Commission.

Dans ce contexte, le présent avant-projet de loi vise à exécuter et à compléter le règlement 910/2014. À cette fin, une loi relative à l'identification électronique est adoptée. Elle prévoit un principe de reconnaissance mutuelle pour des moyens d'identification électronique notifiés par d'autres États membres européens, précise les niveaux de garantie, un mécanisme de surveillance et de contrôle ainsi que des dispositions portant sur la collaboration et l'interopérabilité.

C. IDENTIFICATION ÉLECTRONIQUE POUR APPLICATIONS PUBLIQUES BELGES

La seconde partie de l'avant-projet n'a pas de lien direct avec l'application du règlement 910/2014 mais vise l'introduction d'un cadre juridique pour l'identification électronique dans le contexte des applications publiques belges.

Elle concerne d'une part le fonctionnement du service fédéral d'authentification qui se charge de la gestion de l'identité et de l'accès pour les applications publiques belges. D'autre part, elle prévoit la possibilité d'agréer des moyens d'identification électronique mobiles et non mobiles qui peuvent être utilisés pour accéder à des applications publiques belges. À cette fin, la

voorzien in de nodige bepalingen in deze wet betreffende elektronische identificatie.

loi relative à l'identification électronique prévoit les dispositions nécessaires.

D. ARTIKELSGEWIJZE BESPREKING

D. COMMENTAIRE DES ARTICLES

Hoofdstuk 1. Algemene bepaling

Chapitre 1er. Disposition générale

Artikel 1.

Dit artikel vereist geen bijzondere commentaar.

Article 1er.

Cet article ne requiert aucun commentaire particulier.

Hoofdstuk 2. Definities en toepassingsgebied

Chapitre 2. Définitions et champ d'application

Afdeling 1. Definities

Section 1ère. Définitions

Artikel 2.

Artikel 2 van dit voorontwerp definieert het tweezijdig doel van de wet elektronische identificatie.
Enerzijds past deze wet hoofdstuk II (elektronische identificatie) van verordening 910/2014 toe.
Anderzijds voorziet zij een juridisch kader voor elektronische identificatiemiddelen waarmee toegang kan worden verkregen tot Belgische overheidstoepassingen.

Article 2.

L'article 2 du présent avant-projet définit le but double de la loi relative à l'identification électronique.
D'une part, cette loi applique le chapitre II (identification électronique) du règlement 910/2014.
D'autre part, elle prévoit un cadre juridique pour des moyens d'identification électronique permettant d'accéder à des applications publiques belges.

Artikel 3.

Artikel 3 § 1, 1° van dit voorontwerp bepaalt dat als er sprake is van verordening 910/2014 men de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, bedoelt. Immers, aangezien dit voorontwerp ertoe strekt die verordening toe te passen voor wat hoofdstuk II (elektronische identificatie) betreft, is het nuttig om die term te definiëren, teneinde de tekst leesbaarder te maken, telkens wanneer verwezen wordt naar alle of een gedeelte van de bepalingen van de verordening. Hetzelfde geldt voor de uitvoeringsverordeningen van de verordening 910/2014 waarnaar verwezen wordt.

Article 3.

L'article 3 § 1er, 1° du présent avant-projet prévoit que lorsqu'il est question de « règlement 910/2014 », il s'agit du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. En effet, vu que cet avant-projet vise à appliquer le chapitre II de ce règlement (identification électronique), il est utile de définir ce terme afin de rendre le texte plus lisible, quand il est fait référence à l'ensemble ou à une partie des dispositions du règlement.
Il en va de même pour les règlements d'exécution du Règlement 910/2014 auxquels il est fait référence.

Artikel 3 § 1, 4° van dit voorontwerp definieert het begrip toezichthoudend orgaan. Ook al

L'article 3 § 1er, 4° de l'avant-projet définit le concept de l'organe de contrôle. Même si ce

wordt dit begrip in de verordening 910/2014 niet gehanteerd in de context van hoofdstuk II (elektronische identificatie), volgt uit artikel 9, 1, b) van verordening 910/2014 de plicht voor lidstaten om een toezichtregeling te voorzien voor aangemelde stelsels voor elektronische identificatie. Om te voldoen aan deze verplichting inzake toezichtregeling voorziet dit ontwerp de aanduiding van een toezichthoudend orgaan.

Deze definitie bepaalt enerzijds dat het orgaan bestaat uit experten van de Federale Overheidsdienst Binnenlandse Zaken, van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie en van de Federale Overheidsdienst Informatie- en Communicatietechnologie en anderzijds dat dit orgaan verantwoordelijk is voor het uitoefenen van toezicht op door de overheid aangemelde stelsels voor elektronische identificatie.
Het toezichthoudend orgaan, zoals hier bedoeld, heeft geen enkele bevoegdheid om toezichthoudende taken uit te voeren die betrekking hebben op vertrouwensdiensten.

Paragraaf 2 van artikel 2 vereist geen bijzondere commentaar.

concept n'est pas utilisé dans le règlement 910/2014 dans le contexte du chapitre II (identification électronique), l'obligation pour les États membres de prévoir un régime de contrôle pour les schémas d'identification électronique notifiés découle de l'article 9, 1, b) du règlement 910/2014. Pour satisfaire à cette obligation relative au régime de contrôle, le présent projet prévoit la désignation d'un organe de contrôle.

Cette définition prévoit d'une part que l'organe se compose d'experts du Service public fédéral Intérieur, du Service public fédéral Économie, PME, Classes moyennes et Énergie et du Service public fédéral Technologie de l'Information et de la Communication et d'autre part que cet organe est responsable de l'exercice du contrôle des schémas d'identification électronique notifiés par l'Administration.
L'organe de contrôle dont queston n'a cependant aucune compétence pour exécuter des tâches de contrôle relatives aux services de confiance.

Le paragraphe 2 de l'article 2 ne requiert aucun commentaire particulier.

Afdeling 2. Toepassingsgebied

Artikel 4.

Doordat deze wet twee afzonderlijke en autonome onderwerpen beheerst, moet ook het toepassingsgebied van deze wet voor beide onderdelen afzonderlijk worden gedefinieerd.

Paragraaf 1 van artikel 4 van dit voorontwerp definieert het toepassingsgebied van hoofdstuk 3 van deze wet dat hoofdstuk II (elektronische identificatie) uitvoert en van toepassing is op grensoverschrijdende transacties binnen Europa. De bepalingen van dit hoofdstuk zijn, met uitzondering van artikel 5, enkel van toepassing op stelsels voor elektronische identificatie die door België overeenkomstig artikel 9 van verordening 910/2014 werden aangemeld bij de Commissie als ook op de verantwoordelijken daarvan en op partijen die een elektronisch identificatiemiddel

Section 2. Champ d'application

Article 4.

Comme cette loi concerne deux sujets distincts et autonomes, son champ d'application doit également être défini distinctement pour chacun des sujets.

Le paragraphe 1er de l'article 4 du présent avant-projet définit le champ d'application du chapitre 3 de cette loi qui exécute le chapitre II (identification électronique) et qui s'applique aux transactions transfrontalières au sein de l'Europe. Les dispositions de ce chapitre, à l'exception de l'article 5, ne s'appliquent qu'aux schémas d'identification électronique qui ont été notifiés à la Commission par la Belgique conformément à l'article 9 du règlement 910/2014 ainsi qu'aux leurs responsables et aux parties qui délivrent un moyen d'authentification électronique ou qui gèrent une procédure

uitgeven of die een authenticatieprocedure uitvoeren in het kader van een aangemeld stelsel voor elektronische identificatie.
Paragraaf 2 van artikel 4 van dit voorontwerp bepaalt dat hoofdstuk 4 enkel van toepassing is op diensten voor elektronische identificatie waarmee toegang kan worden verkregen tot Belgische digitale overheidstoepassingen. Elektronische identificatiediensten aangeboden door private organisaties om toegang te krijgen tot private toepassingen (bijvoorbeeld van bankinstellingen) vallen bijgevolg buiten het toepassingsgebied.

De regels vervat in hoofdstuk 4 zijn evenmin een toepassing van de verordening 910/2014. Dat betekent echter niet dat elektronische identificatiemiddelen die worden erkend op grond van hoofdstuk 4 niet kunnen worden aangemeld bij de Commissie, in welk geval de bepalingen van hoofdstuk 3 hiervoor ook relevant worden.

Hoofdstuk 3. Grensoverschrijdende elektronische identificatie

Afdeling 1. Wederzijdse erkenning

Artikel 5.

In de Belgische wetgeving wordt verwezen naar verschillende Belgische elektronische identificatiemiddelen.
Het gebruik van dergelijke begrippen als voorwaarde om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in België, brengt een beperking met zich mee die in het licht van artikel 6 §1 van verordening 910/2014 niet langer gehandhaafd kan worden. Immers, in het licht van dat artikel, moeten ook elektronische identificatiemiddelen uitgegeven in andere lidstaten worden aanvaard om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in België mits aan een aantal voorwaarden is voldaan (waaronder aanmelding bij de Commissie).
Teneinde te vermijden dat alle wetgevende instrumenten, waarin een uiteenlopende terminologie gehanteerd wordt, gewijzigd moeten worden, voert paragraaf 1 van artikel 5 van dit voorontwerp een equivalentie in voor aangemelde elektronische

d'authentification dans le cadre d'un schéma d'identification électronique notifié.
Le paragraphe 2 de l'article 4 du présent avant-projet prévoit que le chapitre 4 ne s'applique qu'aux services pour identification électronique permettant d'accéder à des applications publiques numériques belges. Par conséquence, les services d'identification électronique offerts par des organisations privées pour accéder à des applications privées (par exemple des institutions bancaires) ne font pas partie du champ d'application.

Les règles du chapitre 4 ne constituent pas non plus une application du règlement 910/2014. Cela ne signifie cependant pas que les moyens d'identification électronique reconnus sur la base du chapitre 4 ne peuvent pas être notifiés à la Commission, auquel cas les dispositions du chapitre 3 sont également pertinentes à cette fin.

Chapitre 3. Identification électronique transfrontalière

Section 1ère. Reconnaissance mutuelle

Article 5.

La législation belge évoque différents moyens d'identification électronique belges.

L'utilisation de tels concepts en tant que condition d'accès à un service en ligne offert par une instance publique en Belgique entraîne une restriction qui, à la lumière de l'article 6 §1er du règlement 910/2014, ne peut plus subsister. En effet, à la lumière de cet article, les moyens d'identification électronique délivrés dans d'autres États membres sont reconnus afin d'accéder à un service en ligne offert par une instance publique en Belgique moyennant le respect d'une série de conditions (notamment notification à la Commission).
Afin d'éviter que tous les instruments législatifs, qui utilisent une terminologie disparate, doivent être modifiés, le paragraphe 1er de l'article 5 du présent avant-projet introduit une équivalence pour les moyens d'identification électronique notifiés qui sont délivrés dans un autre État membre.

identificatiemiddelen uitgegeven in een andere lidstaat.

Het belang van deze bepaling kan het best geïllustreerd worden aan de hand van een hypothetisch voorbeeld. Indien de overheid aan de Belgische elektronische identiteitskaart een betrouwbaarheidsniveau 'hoog' toekent en deze aanmeldt bij de Commissie, en de Belgische wetgeving vereist voor de toegang tot de onlinedienst van een bepaalde Belgische openbare instantie het gebruik van *'de door de Belgische overheid uitgereikte elektronische identiteitskaart'* of *'het identiteitscertificaat op de elektronische identiteitskaart'*, zal de desbetreffende Belgische openbare instantie, onafgezien van de bewoordingen van de Belgische wet, ook door andere lidstaten aangemelde elektronische identificatiemiddelen moeten aanvaarden wanneer die voldoen aan het betrouwbaarheidsniveau 'hoog'.
België zal net als andere lidstaten een uniek transnationaal nummer voorzien om zijn burgers te identificeren in een transnationale context.

Lidstaten dienen de private sector aan te moedigen om vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen. Daarom moet de mogelijkheid tot elektronische identificatie die elke lidstaat biedt beschikbaar zijn voor zowel binnen als buiten het grondgebied gevestigde vertrouwende partijen. De lidstaat mag overeenkomstig artikel 7, f), lid 2 van verordening 910/2014 echter voorwaarden stellen voor toegang tot die elektronische identificatie. Paragraaf 2 van dit artikel belast de Koning met het vaststellen van de voorwaarden waaraan private instanties moeten voldoen om toegang te krijgen tot de door de overheid aangeboden online identificatie. Omdat hier allicht een impact is op het vlak van persoonsgegevens zal hierover het advies gevraagd worden van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Afdeling 2. Betrouwbaarheidsniveaus

Artikel 6.

Pour illustrer l'importance de cette disposition, le mieux est de présenter un exemple hypothétique. Si l'administration attribue à la carte d'identité électronique belge un niveau de garantie « élevé » et la notifie à la Commission, et que la législation belge exige pour l'accès au service en ligne d'une instance publique belge déterminée l'utilisation de la *« carte d'identité électronique délivrée par l'Administration belge »* ou du *« certificat d'identité sur la carte d'identité électronique »*, l'instance publique belge en question devra, en dépit des termes de la loi belge, également accepter des moyens d'identification électronique notifiés par d'autres États membres s'ils satisfont au niveau de garantie « élevé ».

La Belgique, tout comme d'autres États membres, prévoira un numéro transnational unique afin d'identifier ses citoyens dans un contexte transnational.

Les États membres doivent encourager le secteur privé à utiliser volontairement des moyens d'identification électronique relevant d'un schéma notifié. Dès lors, la possibilité d'identification électronique offerte par chaque État membre doit être disponible pour les parties utilisatrices établies tant au sein qu'en dehors du territoire. Conformément à l'article 7, f), alinéa 2 du règlement 910/2014, l'État membre peut cependant définir les conditions d'accès à cette identification électronique. Le paragraphe 2 de cet article charge le Roi de fixer les conditions auxquelles des instances privées doivent satisfaire pour accéder à l'identification en ligne offerte par l'administration. Comme l'impact en la matière sur les données à caractère personnel est évident, on demandera à ce sujet l'avis de la Commission de la protection de la vie privée.

Section 2. Niveaux de garantie

Article 6.

Overeenkomstig artikel 6, paragraaf 1, b) van verordening 910/2014, zoals bestendigd in paragraaf 1 van dit artikel, moet elke overheidsdienst bepalen welk betrouwbaarheidsniveau nodig is om toegang te krijgen tot haar diensten. Binnen dat niveau en de hogere niveaus heeft de burger de keuze tussen één of meer identificatiemiddelen om zich dan effectief toegang te verschaffen tot de overheidstoepassing.
Volgens verordening 910/2014 zal de overheidsdienst die binnen de Belgische context de niveaus "substantieel" en "hoog" toelaat ook de Europees aangemelde identificatiemiddelen uit andere lidstaten met een overeenstemmend of hoger betrouwbaarheidsniveau dienen toe te laten voor inwoners van andere Europese lidstaten. Of de persoon al dan niet werkelijk toegang krijgt tot de dienst wordt door de overheidsdienst bepaald.
Daarnaast moeten de betrouwbaarheidsniveaus voor de bij de Commissie aan te melden elektronische identificatiemiddelen bepaald worden in overeenstemming met Uitvoeringsverordening (EU) 2015/1502. Paragraaf 2 van artikel legt de bevoegdheid hiervoor bij de federale overheidsdienst Informatie- en Communicatietechnologie, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut. Deze consultaties zijn nodig om de impact van de bepaling van het betrouwbaarheidsniveau op de business te evalueren. De federale overheidsdienst Informatie- en Communicatietechnologie zorgt in naam van de Belgische overheid voor aanmelding bij de Europese Commissie van één of meerdere Belgische stelsels voor elektronische identificatie overeenkomstig artikel 9 van verordening 910/2014.

Conformément à l'article 6, paraphe 1er, b) du règlement 910/2014, et comme prévu au paragraphe 1er du présent article, chaque service public doit déterminer quel niveau de garantie est nécessaire pour accéder à ses services. Au sein de ce niveau et des niveaux plus élevés, le citoyen a le choix entre un ou plusieurs moyens d'identification pour accéder effectivement à l'application publique.

Selon le règlement 910/2014, le service public qui, dans le contexte belge, autorise les niveaux « substantiel » et « élevé », devra aussi autoriser pour les habitants d'autres États membres européens des moyens d'identification européens notifiés d'autres États membres. Le fait que la personne accède effectivement ou non au service est déterminé par le service public.

Par ailleurs, les niveaux de garantie pour les moyens d'identification électronique à notifier à la Commission doivent être déterminés conformément au Règlement d'exécution (UE) 2015/1502. Le paragraphe 2 de cet article attribue la compétence en la matière au service public fédéral Technologie de l'Information et de la Communication, après consultation du Collège des présidents des service publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux. Ces consultations sont nécessaires afin d' évaluer l'impact de la définition du niveau de garantie sur le business.
Le service public fédéral Technologie de l'Information et de la Communication se charge au nom de l'Etat Belge de la notification à la Commission Européenne d'un ou de plusieurs schémas d'identification électronique belges conformément à l'article 9 du règlement 910/2014

Afdeling 3.
Persoonsidentificatiegegevens en toegang tot het Rijksregister

Artikel 7.

Section 3. Données d'identification personnelle et accès au Registre national

Article 7.

De uitvoeringsverordening (EU) 2015/1501 bevat bepalingen in verband met de uitwisseling en de beveiliging van informatie die dient te worden uitgewisseld tussen de lidstaten in het kader van grensoverschrijdende identificatie.
Zo is er een minimale set persoonsidentificatiegegevens gedefinieerd in artikel 11 en in de bijlage van de hierboven vermelde uitvoeringsverordening. Deze informatie zal worden uitgewisseld wanneer een persoon die houder is van een Belgisch elektronische identificatiemiddel, zich wenst toegang te verschaffen tot online toepassingen in het buitenland. Uiteraard zal de gebruiker hierover geïnformeerd worden.
Dit artikel geeft aan de federale overheidsdienst Informatie- en Communicatietechnologie de opdracht om deze informatie uit te wisselen en hiervoor het Rijksregister te consulteren.
Conform het advies nr 48/2016 van de Commissie voor de bescherming van de persoonlijke levenssfeer, zal bij uitwisseling van gegevens in toepassing van artikel 7, f), tweede lid van de verordening 910/2014 aan niet openbare instanties slechts een beperkt pakket persoonsidentificatiegegevens worden meegestuurd.
Bij nieuwe toekomstige bepalingen die voorzien om facultatieve persoonsidentificatigegevens uit te wisselen conform verordening 910/2014 of één van haar uitvoeringshandelingen, zal eveneens het Rijksregister worden geconsulteerd, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Afdeling 4. Toezicht en controle

Artikel 8.

Overeenkomstig artikel 9, lid 1, b) van verordening 910/2014 geeft de aanmeldende lidstaat de Commissie onverwijld kennis van de toepasselijke toezichtregeling en informatie over de aansprakelijkheidsregeling met betrekking tot de partij die het elektronische identificatiemiddel uitgeeft en de partij die de authenticatieprocedure uitvoert.
Overeenkomstig artikel 9, lid 1, g) van verordening 910/2014 geeft de aanmeldende lidstaat ook onverwijld kennis van de regeling

Le règlement d'exécution (UE) 2015/1501 prévoit des dispositions relatives à l'échange et à la sécurité des informations qui doivent être échangées entre les États membres dans le cadre de l'identification transfrontalière.
Ainsi, un ensemble minimum de données d'identification personnelle a été défini à l'article 11 et à l'annexe du règlement d'exécution susmentionné. Ces informations seront échangées lorsqu'une personne titulaire d'un moyen d'identification électronique belge souhaitera accéder à des applications en ligne à l'étranger. L'utilisateur en sera bien entendu informé.
Le présent article confère au service public fédéral Technologie de l'Information et de la Communication la mission d'échanger ces informations et de consulter le Registre national à cette fin.

Conformément à l'avis n° 48/2016 de la Commission de la protection de la vie privée, l'échange de données, en application de l'article 7, f), deuxième alinéa du règlement 910/2014, avec des instances non publiques n'entraînera la transmission que d'un ensemble minimal de données d'identification personnelle.
En cas de nouvelles dispositions futures qui prévoient l'échange de données d'identification personnelle facultatives conformément au règlement 910/2014 ou à l'un de ses actes d'exécution, le Registre national sera également consulté, après avis de la Commission de la protection de la vie privée.

Section 4. Surveillance et contrôle

Article 8.

Conformément à l'article 9, alinéa 1, b) du règlement 910/2014, l'État membre notifiant notifie dans les meilleurs délais à la Commission le régime de contrôle applicable et des informations sur la responsabilité en ce qui concerne la partie qui délivre le moyen d'identification électronique et la partie qui gère la procédure d'authentification. Conformément à l'article 9, alinéa 1, g) du règlement 910/2014, l'État membre notifiant notifie également dans les meilleurs délais les

voor de opschorting of intrekking van het aangemelde stelsel voor elektronische identificatie of de delen waarvan de integriteit is geschonden.
Een dergelijke regeling ontbreekt vandaag in België. Teneinde te kunnen voldoen aan bovenstaande door verordening 910/2014 gestelde informatieverplichtingen, bepaalt artikel 8 van dit voorontwerp dat een toezichtsorgaan wordt opgericht bestaande uit experten van de Federale Overheidsdienst Binnenlandse Zaken, van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie en van de Federale Overheidsdienst Informatie- en Communicatietechnologie. Het toezicht zal onder andere bestaan uit preventie, monitoring, en controle.

De Verordening voorziet geen orgaan voor het toezicht op de aangemelde schema's voor elektronische identificatie. Het lijkt echter raadzaam dat deze bevoegdheid van toezicht wordt toegewezen aan een orgaan in plaats van ad hoc te bekijken wat de toezichtregeling is.
Wanneer aangewezen kan het toezichthoudend orgaan zich laten bijstaan door deskundigen.
Het toezichthoudend orgaan kan in gebreke blijvende partijen in gebreke stellen en hen verzoeken om de nodige maatregelen te treffen om die tekortkoming te verhelpen en de dienstverlening te verbeteren. Het gaat hierbij over inbreuken waarbij de persoonsgegevens niet in gevaar komen (verlies, ongeoorloofde wijziging, ongeoorloofde toegang, diefstal) want bij inbreuken waarbij de persoonsgegevens in gevaar komen volgt opschorting of intrekking.

Bij gebreke aan de nodige maatregelen door ingebreke blijvende partijen kan de minister of zijn gemachtigde, op advies van het toezichthoudend orgaan, en na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, overgaan tot de intrekking of opschorting van een volledig stelsel van elektronische identificatie of van een gedeelte daarvan.

dispositions concernant la suspension ou la révocation du schéma d'identification électronique notifié ou des parties compromises concernées.

Un tel règlement fait actuellement défaut en Belgique. Afin de pouvoir répondre aux obligations d'information précitées du règlement 910/2014, l'article 8 du présent avant-projet précise qu'un organe de contrôle sera créé et sera composé d'experts du Service public fédéral Intérieur, du Service public fédéral Économie, PME, Classes moyennes et Énergie et du Service public fédéral Technologie de l'Information et de la Communication. Le contrôle consistera notamment en de la prévention, de la surveillance et de la vérification.

Le Règlement ne prévoit pas d'organe pour le contrôle des schémas d'identification électronique notifiés. Il semble néanmoins indiqué d'attribuer cette compétence de contrôle à un organe plutôt que d'examiner ad hoc la réglementation relative au contrôle.
Lorsque c'est indiqué, l'organe de contrôle peut se faire assister par des experts. L'organe de contrôle peut mettre en demeure les parties défaillantes et les inviter à prendre les mesures nécessaires pour combler les défaillances en question et améliorer la prestation de services. Il s'agit d'infractions ne causant pas de préjudice aux données à caractère personnel (perte, modification illicite, accès illicite, vol). En effet, tout préjudice à des données à caractère personnel entraîne une suspension ou une révocation.

À défaut des mesures nécessaires par les parties défaillantes, le ministre ou son mandataire peut, sur conseil de l'organe de contrôle, et après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, procéder à la révocation ou à la suspension d'une partie ou de la totalité d'un schéma d'identification électronique.

Wanneer de integriteit van een aangemeld stelsel in het gedrang is, zal de minister of zijn gemachtigde op advies van het toezichthoudend orgaan, en na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut het stelsel geheel of gedeeltelijk intrekken of opschorten, en de EC en de lidstaten verwittigen.
Het toezichthoudend orgaan zal jaarlijks rapporteren aan de bevoegde ministers.

Lorsque l'intégrité d'un schéma notifié est menacée, le ministre ou son mandataire, sur conseil de l'organe de contrôle, et après consultation du Collège des présidents des services publics fédéraux et de programmation, du Collège des administrateurs délégués des institutions de sécurité sociale et du Collège des administrateurs délégués des organismes fédéraux d'intérêt public, révoquera ou suspendra une partie ou la totalité du schéma et en avertira la Commission européenne ainsi que les États membres.

L'organe de contrôle fera annuellement rapport aux ministres compétents.

Afdeling 5. Samenwerking en interoperabiliteit

Artikel 9.

Overeenkomstig artikel 3 van het Uitvoeringsbesluit 2015/296 van 24 februari 2015 van de Commissie tot vaststelling van procedurele voorschriften betreffende de samenwerking tussen de lidstaten op het gebied van elektronische identificatie overeenkomstig artikel 12, lid 7, van verordening 910/2014, moet de Belgische overheid, teneinde de samenwerking met de andere Europese lidstaten tot stand te brengen, één loket aanwijzen.

Artikel 9 van dit voorontwerp wijst de federale overheidsdienst Informatie- en Communicatietechnologie aan als één loket. De facto vervult de federale overheidsdienst Informatie- en Communicatietechnologie deze rol al.

Artikel 10.

Overeenkomstig artikel 2 van Uitvoeringsverordening 2015/1501 heeft de exploitant van een knooppunt de taak om ervoor te zorgen dat het knooppunt correct en betrouwbaar als aansluitpunt functioneert.

Een knooppunt is een aansluitpunt dat onderdeel is van de interoperabiliteitsarchitectuur voor elektronische identificatie en betrokken is bij

Section 5. Collaboration et interopérabilité

Article 9.

Conformément à l'article 3 de la Décision d'exécution 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement n ° 910/2014, l'administration belge doit désigner un guichet unique afin de mettre en place la coopération entre les États membres européens.

L'article 9 du présent avant-projet désigne le service public fédéral Technologie de l'Information et de la Communication comme guichet unique. De facto, le service public fédéral Technologie de l'Information et de la Communication remplit déjà ce rôle.

Article 10.

Conformément à l'article 2 du règlement d'exécution 2015/1501, l'exploitant d'un nœud doit faire en sorte que les fonctions du nœud en tant que point de connexion soient assurées de manière correcte et fiable.

Un nœud est un point de connexion qui fait partie de l'architecture de l'interopérabilité d'identification électronique et participe au processus d'authentification transfrontalière

de grensoverschrijdende authenticatie van personen, en dat in staat is berichten te herkennen en te verwerken of door te sturen naar andere knooppunten door mogelijk te maken dat de nationale elektronische identificatie-infrastructuur van een lidstaat gekoppeld wordt aan de nationale elektronische identificatie-infrastructuren van andere lidstaten.

Conform de hierboven vermelde Uitvoeringsverordening dienen de knooppunten maatregelen te nemen in verband met de beveiliging van de gegevens.

Artikel 10 van dit voorontwerp wijst de federale overheidsdienst Informatie- en Communicatietechnologie aan als knooppuntexploitant. De facto vervult de federale overheidsdienst Informatie- en Communicatietechnologie deze rol al.

des personnes et qui a la capacité de reconnaître et de traiter ou d'envoyer des transmissions à d'autres nœuds en permettant à l'infrastructure d'identification électronique nationale d'un État membre de fonctionner en interface avec les infrastructures d'identification électronique nationales d'autres États membres.

Conformément au règlement d'exécution susmentionné, les nœuds doivent prendre des mesures relatives à la sécurisation des données.

L'article 10 du présent avant-projet désigne le service public fédéral Technologie de l'Information et de la Communication comme exploitant du nœud. De facto, le service public fédéral Technologie de l'Information et de la Communication remplit déjà ce rôle.

Hoofdstuk 4. Elektronische identificatie voor Belgische overheidstoepassingen

Afdeling 1. Authenticatiedienst

Artikel 11.

Binnen CSAM (een geheel van afspraken en van regels om het identiteits- en toegangsbeheer binnen het e-government te organiseren) baat de federale overheidsdienst Informatie- en Communicatietechnologie een authenticatiedienst ("Federal Authentication Service" of "FAS"), uit, als een essentiële bouwsteen voor e-government. Dit past binnen diens opdracht als horizontale overheidsdienst.
De FAS is een authenticatiedienst gebaseerd op verschillende elektronische identificatiemiddelen om burgers toegang te geven tot digitale overheidstoepassingen met verschillende beveiligingsniveaus die overeenkomstig verordening 910/2014 beoordeeld werden als laag, substantieel en hoog. Er is dus een gelijkstelling met de niveaus zoals die bestaan in de verordening 910/2014 zonder dat er per se enige aanmelding is conform verordening 910/2014. Een ondubbelzinnige wettelijke basis voor de uitbating van de

Chapitre 4. Identification électronique pour applications publiques belges

Section 1ère. Service d'authentification

Article 11.

Au sein de CSAM (un ensemble d'accords et de règles visant à organiser la gestion de l'identité et de l'accès au sein de l'e-gouvernement), le service public fédéral Technologie de l'Information et de la Communication exploite un service d'authentification (« Federal Authentication Service » ou « FAS »), qui constitue un fondement essentiel de l'e-gouvernement. Cette exploitation s'inscrit dans le cadre de sa mission de service public horizontal.
Le FAS est un service d'authentification basé sur différents moyens d'identification électronique permettant aux citoyens d'accéder à des applications publiques numériques assortis de différents niveaux de sécurité qui, conformément au règlement 910/2014, ont été qualifiés de faibles, substantiels et élevés. Il y a donc une équivalence avec les niveaux définis dans le règlement 910/2014 sans qu'aucune notification ne soit faite conformément au règlement 910/2014. Il n'existe actuellement aucune base légale explicite pour

authenticatiedienst ontbreekt tot op heden. Om die reden voorziet artikel 11 van dit voorontwerp in de nodige wettelijke verankering van de federale authenticatiedienst, waarbij ook in de verplichting wordt voorzien om te zorgen voor de beschikbaarheid van de federale authenticatiedienst.
Wanneer de federale overheidsdienst voor Informatie- en Communicatietechnologie dat nodig acht kan zij voor de exploitatie van de authenticatiedienst samenwerken met andere overheidsdiensten en/of met private partners.
Overeenkomstig de beraadslaging RR 21/2015 van het sectoraal comité van het Rijksregister heeft de federale overheidsdienst voor Informatie- en Communicatietechnologie het recht om het rijksregisternummer te gebruiken bij aanwending van de federale authenticatiedienst voor toegangs- en gebruikersbeheer voor informatietoepassingen voor opdrachten van algemeen belang. Het gebruik van het rijksregisternummer is noodzakelijk om de identificatie en de authenticatie van personen correct te laten verlopen. Het gaat om een uniek nummer waarmee een persoon met grote nauwkeurigheid kan worden geïdentificeerd. De federale authenticatiedienst kan zo bijdragen aan het respecteren door de federale instanties van de verplichting in artikel 4 §1 van de wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren. Deze bepaling verplicht federale instanties om bij de uitvoering van hun opdrachten het rijksregisternummer te gebruiken voor de identificatie van natuurlijke personen.

l'exploitation du service d'authentification. C'est la raison pour laquelle l'article 11 du présent avant-projet prévoit l'ancrage légale nécessaire du service fédéral d'authentification, ainsi que l'obligation de veiller à la disponibilité du service fédéral d'authentification.
Lorsque le service public fédéral Technologie de l'Information et de la Communication l'estime nécessaire, il peut, pour l'exploitation du service d'authentification, collaborer avec d'autres services publics fédéraux et/ou avec des partenaires privés.
Conformément à la Délibération RN n° 21/2015 du Comité sectoriel du Registre national, le service public fédéral Technologie de l'Information et de la Communication a le droit d'utiliser le numéro de Registre national dans le cadre du recours au service fédéral d'authentification pour la gestion des accès et des utilisateurs aux applications informatiques développées dans le cadre de missions de service public.
L'utilisation du numéro de Registre national est nécessaire pour procéder correctement à l'identification et à l'authentification de personnes. Il s'agit d'un numéro unique permettant d'identifier une personne avec une grande précision. Le service fédéral d'authentification peut ainsi contribuer au respect par les instances fédérales de l'obligation prévue à l'article 4, 1er, de la loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier. Cette disposition oblige les instances fédérales à utiliser, dans le cadre de l'exécution de leurs missions, le numéro de Registre national pour l'identification des personnes physiques.

Afdeling 2. Erkenning elektronische identificatiemiddelen

Artikel 12.

Momenteel kunnen burgers voor digitale overheidstoepassingen (bijvoorbeeld Tax-on-web) gebruik maken van verschillende

Section 2. Reconnaissance des moyens d'identification électronique

Article 12.

Pour accéder à des applications publiques numériques (par exemple Tax-on-web), les citoyens disposent actuellement de

inlogmogelijkheden (verzameld en gezamenlijk aangeboden binnen de FAS), waaronder de elektronische identificatie op basis van de elektronische identiteitskaart. De elektronische identiteitskaart bevat een handtekeningscertificaat om elektronische handtekeningen te plaatsen en een identiteitscertificaat waarmee men online zijn identiteit kan bewijzen.
Op basis van het identiteitscertificaat kunnen de burgers toegang krijgen tot overheidstoepassingen, niet zelden tot hun eigen gegevens waarover de overheid beschikt.

différentes possibilités d'identification (toutes rassemblées et offertes au sein du FAS), parmi lesquelles l'identification électronique sur la base de la carte d'identité électronique. La carte d'identité électronique contient un certificat de signature permettant d'apposer des signatures électroniques et un certificat d'identité permettant de prouver l'identité en ligne.
Sur la base du certificat d'identité, les citoyens peuvent accéder à des applications publiques et il n'est pas rare qu'ils puissent consulter leurs propres données dont l'administration dispose.

Op dit moment heeft de burger voor online inloggen met de elektronische identiteitskaart meestal een verbonden kaartlezer nodig en onderzoek wijst uit dat niet iedereen over zo'n kaartlezer beschikt. Bovendien moet men voor het gebruik van de kaartlezer eID-software installeren. Het is een eenvoudige handeling maar bouwt toch een drempel in voor het gebruik.

Actuellement, le citoyen qui désire s'identifier en ligne à l'aide de sa carte d'identité électronique a besoin d'un lecteur de cartes filaire. Une enquête montre cependant que tout le monde ne dispose pas d'un tel lecteur de cartes. De plus, l'utilisation du lecteur de cartes nécessite l'installation du logiciel eID. Il s'agit d'une opération simple mais qui représente tout de même un obstacle.

In een snel evoluerende digitale wereld waar de burger op verschillende manieren en vanop verschillende toestellen, met inbegrip van mobiele toestellen zoals tablets en smartphones, in contact wenst te treden met de overheid, staat de overheid voor de uitdaging het groeiend aanbod van digitale overheidstoepassingen eveneens open te stellen voor deze nieuwe mobiele toestellen.

Dans un monde numérique en évolution rapide dans lequel le citoyen souhaite entrer en contact avec l'administration de différentes manières et à partir de plusieurs appareils, y compris des appareils mobiles comme des tablettes et des smartphones, l'administration doit relever le défi consistant à ouvrir à ces nouveaux appareils mobiles l'offre croissante d'applications publiques numériques.

De overheid wenst met dit voorontwerp de identificatiemogelijkheden binnen de federale authenticatiedienst voor digitale overheidstoepassingen uit te breiden en het gebruik van mobiel en niet mobiele identificatie eenvoudiger te maken voor burgers. Een erkenning in België voor opname in de Belgische federale authenticatiedienst staat los van een aanmelding bij de Commissie overeenkomstig verordening 910/2014. Sommige identificatiemiddelen zullen niet aangemeld worden overeenkomstig de verordening 910/2014 maar enkel gebruikt worden binnen de Belgische context.

Par le biais du présent avant-projet, l'administration souhaite étendre les possibilités d'identification au sein du service fédéral d'authentification pour les applications publiques numériques et simplifier l'utilisation des identifications mobiles et non mobiles pour les citoyens. Une reconnaissance en Belgique à des fins d'intégration dans le service fédéral d'authentification belge est indépendante de la notification à la Commission conformément au règlement 910/2014. Certains moyens d'identification ne seront pas notifiés conformément au règlement 910/2014 mais uniquement utilisés dans le contexte belge.

Artikel 12 van dit voorontwerp strekt er in het bijzonder toe een kader te scheppen

L'article 12 du présent avant-projet vise en particulier à créer un cadre dans lequel le

waarbinnen de federale overheidsdienst voor Informatie- en Communicatietechnologie, na consultatie van het College van voorzitters van de Federale en Programmatorische Overheidsdiensten, van het College van afgevaardigd bestuurders van de instellingen van sociale zekerheid en van het College van afgevaardigd bestuurders van de federale instellingen van openbaar nut, authenticatiediensten, al dan niet gebaseerd op mobiele middelen voor elektronische identificatie, kan erkennen zodat deze erkende diensten burgers toegang mogen geven via de federale authenticatiedienst tot digitale overheidstoepassingen in België.

Het doel van een erkenning is dus dat de erkende diensten voor elektronische identificatie, al dan niet betalend, worden opgenomen als één van de inlogmogelijkheden voor Belgische digitale overheidstoepassingen op het toegangsportaal van de federale overheidsdienst Informatie- en Communicatietechnologie.

De door de Koning vast te stellen voorwaarden voor erkenning dienen minstens betrekking te hebben op functionele en technische kenmerken, op respect voor de persoonlijke levenssfeer en invulling van veiligheidsvereisten, op dienstverleningsbeheer en op juridische en economische kenmerken. Er zullen garanties gevraagd worden om te beletten dat gegevens voor andere doeleinden dan identificatie en authenticatie kunnen worden gebruikt. De voorwaarden dienen te worden voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer.

Het geheel van voorwaarden dient gepubliceerd te worden op de website van de federale authenticatiedienst.

De federale overheidsdienst voor Informatie- en Communicatietechnologie kan zich voor de erkenning laten bijstaan door experten indien nodig. Gespecialiseerde experten kunnen bijvoorbeeld ingezet worden om veiligheidsaspecten te checken.

Na erkenning kunnen ook private spelers elektronische identificatiemiddelen voor toegang tot digitale overheidstoepassingen aanbieden onafhankelijk van de overheid maar erkend door de overheid.

service public fédéral Technologie de l'Information et de la Communication peut, après consultation du Collège des présidents des service publics fédéraux et des services publics de programmation, du Collège des administrateurs délégués des institutions de la sécurité sociale et du Collège des administrateurs délégués des organismes d'intérêt public fédéraux, agréer des services d'authentification basés ou non sur des moyens d'identification électronique mobiles afin que ces services agréés puissent permettre aux citoyens d'accéder via le service fédéral d'authentification aux applications publiques numériques en Belgique.

L'agrément a donc pour objectif que les services d'identification électronique agréés, payants ou non, soient repris comme faisant partie des possibilités d'identification pour des applications publiques numériques belges sur le portail d'accès du service public fédéral Technologie de l'Information et de la Communication.

Les conditions d'agrément à fixer par le Roi doivent au moins concerner les caractéristiques fonctionnelles et techniques, le respect de la vie privée et d'exigences de sécurité, la gestion des services ainsi que les caractéristiques juridiques et économiques.

Des garanties seront demandées afin d'empêcher que des données ne soient utilisées à des fins autres que l'identification et l'authentification. Les conditions doivent être soumises à la Commission de la protection de la vie privée.

L'ensemble des conditions doit être publié sur le site web du service fédéral d'authentification.

Le service public fédéral Technologie de l'Information et de la Communication peut, si nécessaire, se faire assister par des experts pour l'agrément. Des experts spécialisés peuvent par exemple être engagés pour vérifier des aspects relatifs à la sécurité.

Après l'agrément, des acteurs privés également peuvent offrir des moyens d'identification électronique indépendants de l'administration mais reconnus par celle-ci, pour accéder à des applications publiques numériques.

Eén van de operationele gevolgen van de erkenning is dat de aanbieder van de erkende aanmeldingsdienst wordt beschouwd als een onderaannemer van de erkennende overheid in de zin van artikel 5, eerste lid, 3°, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen. De onderaannemer van de erkennende overheid is dan in die hoedanigheid gemachtigd om het rijksregisternummer te gebruiken enkel voor het toegangs- en gebruikersbeheer voor overheidstoepassingen via de Federal Authentication Service (FAS). Het gebruik van het rijksregisternummer is dus beperkt tot het uitvoeren van de opdrachten van identificatie en authenticatie voor de federale authenticatiedienst. Voor gebruik van het rijksregisternummer buiten de erkenning door de federale overheidsdienst voor Informatie- en Communicatietechnologie dient uiteraard een aparte machtiging te worden bekomen.
De federale overheidsdienst Informatie- en Communicatietechnologie kan controles uitvoeren om te verifiëren of een erkende dienst aan de voorwaarden voldoet en desgevallend de nodige maatregelen nemen indien dat niet het geval is. Deze maatregelen kunnen bestaan uit het opleggen van maatregelen ter verbetering van de dienstverlening, intrekking of schorsing.
Een eventuele vergoedingsregeling voor betaling van erkende diensten voor elektronische identificatie wordt vastgesteld door de Koning. Zo'n vergoedingsregeling moet zich beperken tot een minimale onkostenvergoeding en houdt rekening met het feit dat een erkende aanbieder al een zekere mate van visibiliteit geniet door haar diensten te mogen aanbieden binnen de FAS.

L'une des conséquences opérationnelles de l'agrément est que le fournisseur du service d'identification agréé est considéré comme sous-traitant de l'autorité d'agrément au sens de l'article 5, alinéa 1, 3°, de la loi du 8 août 1983 organisant un Registre national des personnes physiques. En cette qualité, le sous-traitant de l'autorité d'agrément est dès lors autorisé à utiliser le numéro de Registre national uniquement pour la gestion de l'accès et des utilisateurs sur des applications publiques par le biais du service fédéral d'authentification (FAS). L'utilisation du numéro de Registre national est donc limitée à l'exécution des missions d'identification et authentification pour le service fédéral d'authentification. Pour l'utilisation du numéro de Registre national ne relevant pas de l'agrément par le service public fédéral Technologie de l'Information et de la Communication, il va de soi qu'une autorisation distincte doit être obtenue.

Le service public fédéral Technologie de l'Information et de la Communication peut procéder à des contrôles afin de vérifier si un service agréé répond aux conditions et prendre les cas échéant les mesures nécessaires si ces conditions ne sont pas respectées. Ces mesures peuvent comprendre l'imposition de mesures d'amélioration de la prestation de services, de révocation ou de suspension.
Un éventuel régime d'indemnités relatif au paiement des services d'identification électronique agréés est fixé par le Roi. Un tel régime d'indemnités doit se limiter à un remboursement minimal des frais et tient compte du fait qu'un fournisseur agréé bénéficie déjà d'une certaine mesure de visibilité en étant autorisé à offrir ses services au sein du FAS.

Afdeling 3. Verplichtingen verbonden aan het elektronisch identificatiemiddel

Artikel 13.

In dit artikel wordt gepreciseerd dat de burger die in het bezit is van een elektronisch

Section 3. Obligations liées au moyen d'identification électronique

Article 13.

Cet article précise que le citoyen en possession d'un moyen d'identification électronique a une série d'obligations visant

identificatiemiddel een aantal verplichtingen heeft ter bescherming van zijn elektronische identificatiemiddel. Hij moet zorgen dat hij het middel onder zijn exclusieve controle houdt wat onder meer inhoudt dat paswoorden strikt confidentieel moeten worden gehouden. Hij moet alle nodige maatregelen nemen om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om ingeval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.
Wanneer het elektronisch identificatiemiddel niet meer geldig is of ingetrokken is, mag de houder het niet meer wetens en willens gebruiken.

à protéger son moyen d'identification électronique. Il doit garder le moyen sous son contrôle exclusif, ce qui implique entre autres que les mots de passe doivent être tenus strictement confidentiels. Il doit prendre toutes les mesures nécessaires pour éviter le vol, la perte ou la divulgation de son moyen d'identification électronique et pour le révoquer immédiatement en cas de vol, de perte ou de divulgation.

Lorsque le moyen d'identification électronique n'est plus valable ou est révoqué, le titulaire ne peut plus l'utiliser sciemment.

Hoofdstuk 5. Inwerkingtreding

Artikel 14.

Artikel 14 van dit voorontwerp bepaalt dat de Koning de inwerkingtreding van hoofdstuk 3 zal vastleggen.

Hoofdstuk 3 van dit voorontwerp dient in werking te treden vooraleer de overheid een stelsel voor elektronische identificatie aanmeldt bij de Commissie. Op 29 september 2018 treedt de verplichting voor lidstaten tot wederzijdse erkenning van elektronische identificatiemiddelen in werking waardoor het sterk aangewezen is om voor die datum Hoofdstuk 3 van dit voorontwerp in werking te laten treden.

De inwerkingtreding van hoofdstuk 4 van dit voorontwerp is niet onderhevig aan externe factoren en kan reeds plaatsvinden.

Chapitre 5. Entrée en vigueur

Article 14.

L'article 14 du présent avant-projet précise que le Roi détermine l'entrée en vigueur du chapitre 3.

Le chapitre 3 de cet avant-projet doit entrer en vigueur avant que l'Administration ne notifie un schéma d'identification électronique à la Commission. Le 29 septembre 2018, l'obligation pour les États membres de reconnaissance mutuelle des moyens d'identification électronique entrera en vigueur. Il est dès lors fortement indiqué de faire entrer en vigueur avant cette date le chapitre 3 du présent avant-projet.

L'entrée en vigueur du chapitre 4 du présent avant-projet n'est pas soumise à des facteurs externes et peut déjà avoir lieu.