RÈGLEMENT D'EXÉCUTION (UE) 2015/1502 DE LA COMMISSION

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 (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 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 [1], et notamment son article 8, paragraphe 3,

considérant ce qui suit:

(1) L'article 8 du règlement (UE) nº 910/2014 prévoit qu'un schéma d'identification électronique notifié en vertu de l'article 9, paragraphe 1, doit préciser les niveaux de garantie (faible, substantiel et élevé) des moyens d'identification électronique délivrés dans le cadre dudit schéma.

(2) Il est indispensable de déterminer les spécifications techniques, normes et procédures minimales afin d'assurer une compréhension commune des détails des niveaux de garantie et d'assurer l'interopérabilité lors de l'établissement des correspondances entre les différents niveaux de garantie nationaux des schémas d'identification électronique notifiés par rapport aux niveaux de garantie visés à l'article 8, ainsi que le prévoit l'article 12, paragraphe 4, point b), du règlement (UE) nº 910/2014.

(3) Les spécifications et les procédures établies dans le présent acte d'exécution se fondent notamment sur la norme internationale ISO/CEI 29115, qui est la principale norme internationale disponible dans le domaine des niveaux de garantie pour les moyens d'identification électronique. Toutefois, la teneur du règlement (UE) nº 910/2014 diffère de celle de cette norme internationale, en particulier eu égard aux exigences de preuve et de vérification d'identité, ainsi qu'à la façon dont les différences entre les règles des États membres en matière d'identité et les outils existants dans l'Union européenne aux mêmes fins sont prises en compte. Par conséquent, bien que l'annexe se fonde sur cette norme internationale, elle ne devrait pas faire référence à un quelconque contenu spécifique de la norme ISO/CEI 29115.

(4) L'élaboration du présent règlement résulte d'une approche axée sur les résultats, considérée comme étant la plus appropriée, ce qui transparaît également dans les définitions utilisées pour spécifier les termes et concepts. L'objectif du règlement (UE) nº 910/2014 eu égard aux niveaux de garantie des moyens d'identification électronique est pris en considération. Par conséquent, il convient de tenir le plus grand compte du projet pilote à grande échelle STORK, et notamment des spécifications élaborées dans le cadre de ce projet, ainsi que des définitions et des concepts figurant dans la norme ISO/CEI 29115, pour établir les spécifications et les procédures énumérées dans le présent acte d'exécution.

(5) Selon le contexte dans lequel un aspect donné d'un élément d'identification doit être vérifié, les sources faisant autorité peuvent prendre différentes formes, telles que des registres, documents et organismes. Les sources faisant autorité peuvent être différentes selon les États membres, même dans un contexte similaire.

(6) Les exigences de preuve et de vérification d'identité devraient tenir compte des différents schémas et pratiques, tout en assurant un niveau de garantie suffisamment élevé pour établir la confiance nécessaire. Par conséquent, toute acceptation de procédures utilisées précédemment dans un but autre que la délivrance de moyens d'identification électronique devrait être subordonnée à la confirmation que ces procédures remplissent les conditions prévues pour le niveau de garantie correspondant.

[1] JO L 257 du 28.8.2014, p. 73.

(7) Certains facteurs d'authentification, tels que les secrets partagés, les dispositifs physiques et les caractéristiques physiques, sont généralement employés. Toutefois, il y a lieu d'encourager l'utilisation d'un plus grand nombre de facteurs d'authentification, notamment relevant de catégories différentes, pour renforcer la sécurité du processus d'authentification.

(8) Le présent règlement ne devrait pas affecter les droits de représentation des personnes morales. Toutefois, l'annexe devrait prévoir des exigences concernant l'établissement d'un lien entre les moyens d'identification électronique des personnes physiques et morales.

(9) Il convient de reconnaître l'importance des schémas de gestion de la sécurité de l'information et des services, ainsi que celle de l'utilisation de méthodes reconnues et de l'application des principes inscrits dans des normes comme ISO/CEI 27000 et la série ISO/CEI 20000.

(10) Il convient également de tenir compte des bonnes pratiques relatives aux niveaux de garantie dans les États membres.

(11) La certification de la sécurité informatique basée sur des normes internationales est un outil important pour vérifier que les produits respectent les exigences du présent acte d'exécution.

(12) Le comité visé à l'article 48 du règlement (UE) n° 910/2014 n'a pas rendu d'avis dans le délai fixé par son président,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

1. Les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié sont déterminés par référence aux spécifications et procédures figurant à l'annexe.

2. Les spécifications et procédures figurant à l'annexe doivent être utilisées pour spécifier le niveau de garantie des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié en déterminant la fiabilité et la qualité des éléments suivants:

a) inscription, conformément aux dispositions du point 2.1 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, point a), du règlement (UE) n° 910/2014;

b) gestion des moyens d'identification électronique, conformément aux dispositions du point 2.2 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, points b) et f), du règlement (UE) n° 910/2014;

c) authentification, conformément aux dispositions du point 2.3 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, point c), du règlement (UE) n° 910/2014;

d) gestion et organisation, conformément aux dispositions du point 2.4 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, points d) et e), du règlement (UE) n° 910/2014.

3. Lorsque les moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié répondent à une exigence énoncée pour un niveau de garantie plus élevé, ils sont réputés respecter l'exigence équivalente d'un niveau de garantie inférieur.

4. Sauf indication contraire dans la partie pertinente de l'annexe, un moyen d'identification électronique délivré dans le cadre d'un schéma d'identification électronique notifié doit, pour correspondre à un niveau de garantie donné, comporter tous les éléments énumérés à l'annexe en ce qui concerne ce niveau de garantie.

Article 2

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 8 septembre 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE

Spécifications techniques et procédures pour les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié

1. Définitions applicables

Aux fins de la présente annexe, on entend par:

1) «source faisant autorité», toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité;

2) «facteur d'authentification», un facteur confirmé comme étant lié à une personne, qui relève de l'une des catégories suivantes:

   a) «facteur d'authentification basé sur la possession», un facteur d'authentification dont il revient au sujet de démontrer la possession;

   b) «facteur d'authentification basé sur la connaissance», un facteur d'authentification dont il revient au sujet de démontrer la connaissance;

   c) «facteur d'authentification inhérent», un facteur d'authentification qui est basé sur un attribut physique d'une personne physique, et dont il revient au sujet de démontrer qu'il possède cet attribut physique;

3) «authentification dynamique», un processus électronique utilisant la cryptographie ou d'autres techniques pour fournir un moyen permettant de créer sur demande une preuve électronique attestant que le sujet contrôle ou possède les données d'identification et qui change avec chaque authentification entre le sujet et le système vérifiant l'identité du sujet;

4) «système de gestion de la sécurité de l'information», un ensemble de processus et de procédures visant à gérer les risques associés à la sécurité de l'information pour les maintenir à des niveaux acceptables.

2. Spécifications techniques et procédures

Les éléments des spécifications techniques et des procédures décrits dans la présente annexe servent à déterminer de quelle façon les exigences et les critères de l'article 8 du règlement (UE) n° 910/2014 sont appliqués aux moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique.

2.1. *Inscription*

2.1.1. Demande et enregistrement

Niveau de garantie	Éléments nécessaires
Faible	1. S'assurer que le demandeur est informé des conditions associées à l'utilisation du moyen d'identification électronique. 2. S'assurer que le demandeur est informé des précautions de sécurité recommandées relatives au moyen d'identification électronique. 3. Recueillir les données d'identité pertinentes requises pour la preuve et la vérification d'identité.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.1.2. Preuve et vérification d'identité (personne physique)

Niveau de garantie	Éléments nécessaires
Faible	1. La personne peut être présumée en possession d'un élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et représentant l'identité alléguée. 2. L'élément d'identification peut être présumé authentique ou on peut présumer qu'il existe selon une source faisant autorité et cet élément semble être valide. 3. L'existence de l'identité alléguée est connue d'une source faisant autorité et on peut présumer que la personne est bien celle qu'elle prétend être.
Substantiel	Niveau faible, plus l'une des options énumérées aux points 1 à 4 ci-après: 1. Il a été vérifié que la personne est en possession d'un élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et représentant l'identité alléguée et l'élément d'identification fait l'objet d'une vérification visant à déterminer son authenticité ou l'existence de cet élément est connue d'une source faisant autorité et il se rapporte à une personne réelle et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification; ou 2. une pièce d'identité est présentée au cours d'un processus d'enregistrement dans l'État membre où la pièce d'identité a été délivrée et la pièce d'identité semble se rapporter à la personne qui la présente et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de la pièce d'identité; ou 3. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.2 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 du Parlement européen et du Conseil [1] ou par un organisme équivalent; ou 4. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel et tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent.

Niveau de garantie	Éléments nécessaires
Élevé	Les exigences du point 1 ou 2 ci-dessous doivent être respectées: 1. Niveau substantiel, plus l'une des options énumérées aux points a) à c) ci-dessous: a) Lorsqu'il a été vérifié que la personne est en possession d'un élément d'identification biométrique ou photographique reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et que cet élément correspond à l'identité alléguée, l'élément fait l'objet d'une vérification visant à déterminer sa validité selon une source faisant autorité et le demandeur est identifié comme ayant l'identité alléguée par comparaison d'une ou de plusieurs caractéristiques physiques de la personne auprès d'une source faisant autorité; ou b) lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.2 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats des procédures antérieures demeurent valides; ou c) lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides; OU 2. lorsque le demandeur ne présente pas d'élément d'identification biométrique ou photographique reconnu, les mêmes procédures que celles utilisées au niveau national dans l'État membre de l'entité responsable de l'inscription afin d'obtenir ledit élément d'identification biométrique ou photographique reconnu sont appliquées.

([1]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

2.1.3. Preuve et vérification d'identité (personne morale)

Niveau de garantie	Éléments nécessaires
Faible	1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique.

Niveau de garantie	Éléments nécessaires
	2. L'élément d'identification semble être valide et on peut présumer qu'il est authentique ou qu'il existe selon une source faisant autorité, l'inscription d'une personne morale auprès de la source faisant autorité étant une démarche volontaire et régie par un accord entre la personne morale et la source faisant autorité. 3. La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir en qualité de personne morale.
Substantiel	Niveau faible, plus l'une des options énumérées aux points 1 à 3 ci-après: 1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et (le cas échéant) son numéro d'immatriculation et l'élément d'identification est soumis à une vérification visant à déterminer s'il est authentique, ou si son existence est connue d'une source faisant autorité, l'inscription de la personne morale auprès de la source faisant autorité étant requise pour que la personne morale puisse exercer ses activités dans son secteur et des mesures ont été prises pour minimiser le risque que l'identité de la personne morale ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration des documents; ou 2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.3 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent; ou 3. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent.
Élevé	Niveau substantiel, plus l'une des options énumérées aux points 1 à 3 ci-après: 1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et au moins un identifiant unique représentant la personne morale utilisé dans un contexte national et l'élément d'identification est soumis à une vérification visant à déterminer s'il est valide selon une source faisant autorité; ou

Niveau de garantie	Éléments nécessaires
	2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.3 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette procédure antérieure demeurent valides; ou 3. lorsque les moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides.

2.1.4. Lien établi entre les moyens d'identification électronique de personnes physiques et morales

Le cas échéant, pour établir un lien entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale («lien établi»), les conditions suivantes s'appliquent:

1) Il doit être possible de suspendre et/ou de révoquer le lien établi. Le cycle de vie d'un lien établi (par exemple activation, suspension, renouvellement, révocation) doit être géré selon des procédures reconnues à l'échelle nationale.

2) La personne physique dont le moyen d'identification électronique est lié au moyen d'identification électronique de la personne morale peut déléguer l'établissement du lien à une autre personne physique sur la base de procédures reconnues à l'échelle nationale. Toutefois, la personne physique délégante reste responsable.

3) L'établissement du lien s'effectue comme suit:

Niveau de garantie	Éléments nécessaires
Faible	1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau faible ou supérieur. 2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale. 3. La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir au nom de la personne morale.
Substantiel	Point 3 du niveau faible, plus: 1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau substantiel ou élevé.

Niveau de garantie	Éléments nécessaires
	2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale, qui ont abouti à l'enregistrement du lien établi auprès d'une source faisant autorité. 3. Le lien établi a été vérifié sur la base d'informations provenant d'une source faisant autorité.
Élevé	Point 3 du niveau faible et point 2 du niveau substantiel, plus: 1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau élevé. 2. Le lien a été vérifié sur la base d'un identifiant unique représentant la personne morale et utilisé dans le contexte national; et sur la base d'informations représentant de façon unique la personne physique et provenant d'une source faisant autorité.

2.2. *Gestion des moyens d'identification électronique*

2.2.1. Caractéristiques et conception des moyens d'identification électronique

Niveau de garantie	Éléments nécessaires
Faible	1. Le moyen d'identification électronique utilise au moins un facteur d'authentification. 2. Le moyen d'identification électronique est conçu pour que l'émetteur prenne des mesures raisonnables afin de vérifier qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.
Substantiel	1. Le moyen d'identification électronique utilise au moins deux facteurs d'authentification de différentes catégories. 2. Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.
Élevé	Niveau substantiel, plus: 1. Le moyen d'identification électronique protège contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé. 2. Le moyen d'identification électronique est conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée.

2.2.2. Délivrance, mise à disposition et activation

Niveau de garantie	Éléments nécessaires
Faible	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il ne sera reçu que par le destinataire prévu.
Substantiel	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il sera exclusivement remis en la possession de la personne à laquelle il appartient.
Élevé	Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement en la possession de la personne à laquelle il appartient.

2.2.3. Suspension, révocation et réactivation

Niveau de garantie	Éléments nécessaires
Faible	1. Il est possible de suspendre et/ou de révoquer un moyen d'identification électronique de manière rapide et efficace. 2. Des mesures ont été prises pour prévenir toute suspension, révocation et/ou réactivation non autorisées. 3. La réactivation ne pourra avoir lieu que si les exigences de garantie établies avant la suspension ou la révocation sont toujours respectées.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.2.4. Renouvellement et remplacement

Niveau de garantie	Éléments nécessaires
Faible	En tenant compte des risques d'une modification des données d'identification personnelles, le renouvellement ou le remplacement doit satisfaire aux mêmes exigences de garantie que la preuve et la vérification d'identité initiales ou reposer sur un moyen d'identification électronique valide ayant un niveau de garantie identique ou supérieur.
Substantiel	Identique au niveau faible.
Élevé	Niveau faible, plus: Lorsque le renouvellement ou le remplacement est basé sur un moyen d'identification électronique valide, les données d'identité sont vérifiées auprès d'une source faisant autorité.

2.3. *Authentification*

La présente section met l'accent sur les menaces liées à l'utilisation du mécanisme d'authentification et répertorie les exigences applicables à chaque niveau de garantie. Dans la présente section, les contrôles sont censés être proportionnés aux risques au niveau donné.

2.3.1. Mécanisme d'authentification

Le tableau suivant définit les exigences par niveau de garantie eu égard au mécanisme d'authentification employé par la personne physique ou morale pour utiliser le moyen d'identification électronique destiné à confirmer son identité à une partie utilisatrice.

Niveau de garantie	Éléments nécessaires
Faible	1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité. 2. Lorsque des données d'identification personnelle sont mémorisées dans le cadre du mécanisme d'authentification, ces informations sont sécurisées afin d'assurer leur protection contre toute perte ou compromission, y compris une analyse hors ligne. 3. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque de base renforcé puissent nuire aux mécanismes d'authentification.

Niveau de garantie	Éléments nécessaires
Substantiel	Niveau faible, plus: 1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique. 2. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.
Élevé	Niveau substantiel, plus: Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque élevé puissent nuire aux mécanismes d'authentification.

2.4. *Gestion et organisation*

Tous les participants fournissant un service lié à l'identification électronique dans un contexte transfrontalier («fournisseurs») doivent disposer de pratiques de gestion de la sécurité de l'information documentées, de politiques, d'approches de la gestion des risques et d'autres contrôles reconnus afin de garantir aux organes de gouvernance appropriés responsables des schémas d'identification électronique dans les différents États membres que des pratiques efficaces sont en place. Tous les éléments/exigences figurant au point 2.4 sont censés être proportionnés aux risques au niveau donné.

2.4.1. Dispositions générales

Niveau de garantie	Éléments nécessaires
Faible	1. Les fournisseurs fournissant un service opérationnel visé par le présent règlement sont une autorité publique ou une personne morale reconnue comme telle par le droit national d'un État membre, avec une organisation établie et pleinement opérationnelle à tous les égards pertinents pour la fourniture des services. 2. Les fournisseurs respectent toute exigence légale qui leur incombe dans le cadre du fonctionnement et de l'exécution du service, y compris les types d'informations pouvant être recherchés, la façon dont la preuve d'identité est établie, le type d'informations pouvant être conservées et leur durée de conservation. 3. Les fournisseurs sont en mesure de démontrer leur capacité à assumer la responsabilité d'éventuels dommages, ainsi que le fait qu'ils disposent de ressources financières suffisantes pour la poursuite de leurs activités et la fourniture des services. 4. Les fournisseurs sont responsables de l'exécution de toute tâche sous-traitée à une autre entité, ainsi que du respect de la politique du schéma, comme s'ils s'étaient acquittés eux-mêmes de leur mission. 5. Les schémas d'identification électronique non constitués par le droit national doivent mettre en place un plan de cessation d'activités efficace. Ce plan comporte des mesures concernant l'organisation en cas d'arrêt de fourniture du service ou de la reprise de la fourniture par un autre fournisseur, la façon dont les autorités compétentes et les utilisateurs finaux sont informés, ainsi que des détails sur les modalités de protection, conservation et destruction des informations conformément à la politique du schéma.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.2. Avis publiés et information des utilisateurs

Niveau de garantie	Éléments nécessaires
Faible	1. Il doit exister une définition de service publiée qui inclut toutes les modalités, conditions et frais, y compris les éventuelles limitations de son utilisation. La définition de service doit inclure une politique de confidentialité. 2. Il convient de mettre en place des procédures et politiques appropriées permettant de garantir que les utilisateurs du service sont informés de façon fiable et rapide de tout changement apporté à la définition de service et à toute modalité, condition et politique de confidentialité relative au service spécifié. 3. Il y a lieu de mettre en place des procédures et politiques appropriées permettant d'apporter des réponses complètes et exactes aux demandes de renseignements.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.3. Gestion de la sécurité de l'information

Niveau de garantie	Éléments nécessaires
Faible	Il existe un système de gestion de la sécurité de l'information efficace pour la gestion et le contrôle des risques de sécurité de l'information.
Substantiel	Niveau faible, plus: Le système de gestion de la sécurité de l'information adhère à des normes ou principes éprouvés pour la gestion et le contrôle des risques de sécurité de l'information.
Élevé	Identique au niveau substantiel.

2.4.4. Conservation d'informations

Niveau de garantie	Éléments nécessaires
Faible	1. Enregistrer et conserver les informations pertinentes à l'aide d'un système efficace de gestion des informations, en tenant compte de la législation applicable et des bonnes pratiques en matière de protection et de conservation des données. 2. Conserver, autant qu'il est permis par la législation nationale ou par tout autre arrangement administratif national, et protéger les informations pendant aussi longtemps qu'elles sont nécessaires pour auditer et enquêter sur les atteintes à la sécurité, et à des fins de conservation, après quoi les informations doivent être détruites en toute sécurité.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.5. Installations et personnel

Le tableau suivant présente les exigences relatives aux installations, au personnel et aux sous-traitants, le cas échéant, qui se chargent des tâches visées par le présent règlement. Le respect de chacune des exigences doit être proportionné au niveau de risque associé au niveau de garantie fourni.

Niveau de garantie	Éléments nécessaires
Faible	1. Il existe des procédures garantissant que le personnel et les sous-traitants sont suffisamment formés, qualifiés et expérimentés eu égard aux compétences nécessaires pour exécuter les tâches qui leur sont confiées. 2. Le personnel et les sous-traitants doivent être en nombre suffisant pour faire fonctionner et gérer de manière adéquate le service conformément à ses politiques et procédures. 3. Les installations utilisées pour fournir le service sont surveillées en permanence et protégées contre les dommages causés par des événements environnementaux, l'accès non autorisé et d'autres facteurs susceptibles d'avoir une incidence sur la sécurité du service. 4. Les installations utilisées pour fournir le service garantissent que l'accès aux zones de conservation ou de traitement d'informations personnelles, cryptographiques ou autres informations sensibles est limité au personnel ou aux sous-traitants autorisés.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.6. Contrôles techniques

Niveau de garantie	Éléments nécessaires
Faible	1. Il existe des contrôles techniques proportionnés pour gérer les risques menaçant la sécurité des services, en protégeant la confidentialité, l'intégrité et la disponibilité de l'information traitée. 2. Les canaux de communication électronique utilisés pour échanger des informations personnelles ou sensibles sont protégés contre les écoutes clandestines, la manipulation et le rejeu. 3. L'accès à du matériel cryptographique sensible, si ce dernier est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est limité aux rôles et aux applications pour lesquels il est strictement nécessaire. Il convient de s'assurer que ce matériel n'est jamais conservé de manière permanente en texte clair. 4. Il existe des procédures permettant de garantir que la sécurité est maintenue sur la durée et qu'il est possible de réagir aux changements des niveaux de risque, incidents et atteintes à la sécurité. 5. Tous les supports contenant des informations personnelles, cryptographiques ou autres informations sensibles sont stockés, transportés et mis au rebut de façon sécurisée.
Substantiel	Identique au niveau faible, plus: Le matériel cryptographique sensible, s'il est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est protégé contre toute manipulation non autorisée.
Élevé	Identique au niveau substantiel.

2.4.7. Conformité et audit

Niveau de garantie	Éléments nécessaires
Faible	Il existe des audits internes périodiques dont le champ couvre tous les aspects relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.

Niveau de garantie	Éléments nécessaires
Substantiel	Il existe des audits internes ou externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.
Élevé	1. Il existe des audits externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes. 2. Lorsqu'un schéma est directement géré par un organisme gouvernemental, il est audité conformément au droit national.