Décret n° 2017- XXXX du JJ/MM/2017

fixant le cahier des charges du moyen d'identification électronique présumé fiable

NOR : XXX

***Publics concernés** : particuliers, professionnels, administrations.*

***Objet** : cahier des charges permettant d'établir la présomption de fiabilité attachée à un moyen d'identification électronique, telle que prévu à l'article L.136 du code des postes et des communications électroniques.*

***Entrée en vigueur** : le présent décret entre en vigueur [à préciser].*

***Notice** : L'article 86-I de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique prévoit de compléter le titre Ier du livre III du code des postes et des communications électroniques par un nouvel article L.136. Ce dernier prévoit que la preuve de l'identité aux fins d'accéder à un service de communication en ligne peut être apportée par un moyen d'identification électronique et que ce dernier est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux prescriptions du cahier des charges établi par l'autorité nationale de sécurité des systèmes d'information. Le présent décret fixe le contenu de ce cahier des charges et établit le niveau de fiabilité exigé du moyen d'identification électronique aux fins de bénéficier de la présomption légale de fiabilité telle que visée à l'article L.136, alinéa 2 du code des postes et des communications électroniques.*

***Références** : article L.136 du code des postes et des communications électroniques dans sa rédaction issue de l'article 86-I de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.*

Le Premier ministre,

Sur rapport du Ministre de l'économie et des finances,

Vu 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 ;

Vu le 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) 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 ;

Vu la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique et notamment son article 86-I ;

Vu le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;

Vu le code des postes et des communications électroniques et notamment son article L. 136 ;

Vu le Code de la consommation et notamment son article L.111-1 ;

Vu l'avis rendu par la Commission nationale de l'informatique et des libertés en date du jj/mm/aaaa ;

Vu la notification à la Commission européenne n° XXX du jj/mm/aaaa;

Le Conseil d'État (section de XXX) entendu,

Décrète :

Article 1

Le livre III de la partie règlementaire - décrets en Conseil d'Etat du code des postes et des communications électroniques est complété par un chapitre II ainsi rédigé :

« Chapitre II - Services d'identification électronique

« Section 1 - Présomption de fiabilité

« Article R.54.1 En application du deuxième alinéa de l'article L.136, un moyen d'identification électronique est présumé fiable jusqu'à preuve du contraire s'il est conforme au cahier des charges établi par l'Agence nationale de sécurité des systèmes d'information tel que défini en annexe au présent code (Annexe 1).

« Article R.54.2 L'Agence nationale de la sécurité des systèmes d'information veille à l'adéquation des prescriptions du cahier des charges avec l'état de l'art des technologies et publie en ligne les référentiels techniques déclinant ces prescriptions. »

« Section 2 - Certification du moyen d'identification électronique

« Art R.54.3 L'Agence nationale de la sécurité des systèmes d'information est l'autorité compétente pour certifier la conformité des moyens d'identification électronique et des entités délivrant des moyens d'identification électronique aux exigences du cahier des charges visé à l'article R.54.1 fixant les prescriptions du moyen d'identification électronique présumé fiable. »

Article 2

Le ministre de l'économie et des finances est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le

Par le Premier ministre

Bernard Cazeneuve

Le ministre de l'économie et des finances

Michel Sapin

ANNEXE 1 (Article R.54.1)

Cahier des charges fixant les prescriptions du moyen d'identification électronique présumé fiable conformément au deuxième alinéa de l'article L.136 du code des postes et des communications électroniques

Article 1

Les termes employés dans le présent cahier des charges renvoient aux définitions suivantes :

« Demandeur », la personne, physique ou morale, souhaitant acquérir un moyen d'identification électronique, et dont l'identité reste à prouver ainsi que, éventuellement, la légitimité à effectuer cette démarche.

« Fournisseur du moyen d'identification électronique », la personne morale, publique ou privée, délivrant au demandeur le moyen d'identification électronique.

« Référentiel général de sécurité », le référentiel pris en application du décret n° 2010-112 du 2 février 2010, lui-même pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-156 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

« Norme ISO 17021 », la norme internationale ISO/IEC 17021 intitulée « Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences », dans sa version du 15 juin 2015.

« Norme ISO 27001 », la norme internationale de système de gestion de la sécurité de l'information ISO/IEC 27001 intitulée « Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences », dans sa version du 1er octobre 2013.

« Règlement (UE) n° 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.

« Règlement d'exécution (UE) 2015/1502 », le 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) n° 910/2014.

« Authentification », *« Identification électronique »* et *« Moyen d'identification électronique »* ont la signification qui leur est donnée dans l'article 3 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.

« Source faisant autorité », a la signification qui lui est donnée au paragraphe 1(1) de l'annexe du 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) n° 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.

« Registre », une base contenant des éléments d'identification des personnes physiques ou morales.

Article 2

Un moyen d'identification électronique est présumé fiable jusqu'à preuve du contraire s'il répond aux spécifications techniques et procédures minimales du niveau de garantie élevé tel que défini par le règlement d'exécution (UE) 2015/1502 et s'il remplit les conditions visées aux articles 4 à 13 du présent cahier des charges.

Article 3

Les moyens d'identification électronique présumés fiables jusqu'à preuve du contraire sont valides pour une durée maximale de cinq ans à compter de leur date de délivrance. Cette validité peut être prolongée pour une durée supplémentaire de cinq ans sous réserve d'une nouvelle vérification d'identité du demandeur effectuée conformément aux conditions du présent cahier des charges.

Chapitre I
« Sources faisant autorité »

Article 4

Un registre, y compris s'il a été fourni par un prestataire de services privé, peut être utilisé comme source faisant autorité sous réserve que les processus de saisie mis en place pour ce registre soient suffisamment fiables et garantissent la qualité des données, et que l'entité fournissant le registre soit considérée comme fiable et digne de confiance au niveau national.

Dans le cas où le moyen d'identification électronique est délivré à une personne physique, et lorsque le registre utilisé comme source faisant autorité n'est pas fourni par le fournisseur du moyen d'identification électronique, une convention est conclue entre celui-ci et l'organisme en charge dudit registre, prévoyant notamment que ce dernier est assujetti à toute opération d'audit interne ou externe nécessaire dans le cadre de l'évaluation du niveau de fiabilité présenté par le moyen d'identification électronique.

Article 5

Sont reconnues comme sources faisant autorité pour la preuve et la vérification d'identité des personnes physiques :

- les documents officiels d'identité [tels que listés par le ministère de l'‘intérieur] en cours de validité délivrés par l'Etat français et comportant une photographie d'identité ;
- les documents officiels d'identité en cours de validité délivrés par les Etats membres de l'Union européenne, sous réserve que l'Etat membre concerné rende publiques les caractéristiques de sécurité permettant la vérification de l'authenticité de ces documents et que les informations portées sur ces documents soient présentes en langue anglaise ou française ;
- les passeports émis par des pays situés hors de l'Union européenne faisant l'objet d'une dispense de l'obligation de visa, sous réserve que le pays concerné mette à disposition les moyens nécessaires à la vérification de validité du titre. Si la dispense de l'obligation de visa est assortie de l'obligation de disposer d'un passeport biométrique, alors seul le passeport biométrique est reconnu comme source faisant autorité pour le pays concerné.

Chapitre II
Preuve et vérification d'identité des personnes physiques et des personnes morales

Article 6

Lorsque les procédures précédemment utilisées par une entité publique ou privée dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée pour le niveau de garantie élevé prévu par le règlement (UE) n° 910/2014, l'entité responsable de l'enregistrement de la personne physique ou morale en vue de la délivrance d'un moyen d'identification électronique n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par l'Agence nationale de la sécurité des systèmes d'information.

Article 7

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 prévu par le règlement (UE) n° 910/2014, 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, sous réserve que la délivrance du moyen d'identification électronique servant de base à cette délivrance ait été effectuée en application d'une des autres méthodes de vérification d'identité prévues dans le règlement d'exécution (UE) 2015/1502. Il doit exister une preuve du respect de cette exigence.

Si le moyen d'identification électronique sur lequel est fondée la demande du nouveau moyen d'identification électronique n'a pas fait l'objet d'une notification dans les conditions prévues par le règlement (UE) n° 910/2014, la satisfaction des exigences correspondant au niveau de garantie « élevé » prévu par le règlement (UE) n° 910/2014 doit être confirmée par l'Agence nationale de sécurité des systèmes d'information.

Chapitre III
Caractéristiques et conception des moyens d'identification électronique

Article 8

Afin d'être présumé fiable, le moyen d'identification électronique doit apporter une protection contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé et être conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée.

Les moyens d'identification électronique doivent faire l'objet d'une qualification par l'Agence nationale de la sécurité des systèmes d'information attestant de leur conformité au niveau renforcé du référentiel général de sécurité.

Chapitre IV
Renouvellement et remplacement des moyens d'identification électronique

Article 9

Lorsque des moyens d'identification électronique sont renouvelés ou remplacés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie « élevé » prévu par le règlement (UE) n° 910/2014, 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, sous réserve que la délivrance du moyen d'identification électronique servant de base à ce renouvellement ou ce remplacement ait été effectuée en application d'une des autres méthodes de vérification d'identité prévues dans le règlement d'exécution (UE) 2015/1502. Il doit exister une preuve du respect de cette exigence.

Si le moyen d'identification électronique sur lequel est fondée la demande du nouveau moyen d'identification électronique n'a pas fait l'objet d'une notification dans les conditions prévues par le règlement (UE) n° 910/2014, la satisfaction des exigences correspondant au niveau de garantie « élevé » prévu par le règlement (UE) n° 910/2014 doit être confirmée par l'Agence nationale de sécurité des systèmes d'information.

Chapitre V
Authentification

Article 10

Les modules cryptographiques utilisés pour l'authentification doivent avoir fait l'objet d'une qualification par l'Agence nationale de la sécurité des systèmes d'information attestant de leur conformité au niveau renforcé du référentiel général de sécurité et doivent être utilisés conformément aux conditions d'utilisation définies dans leur attestation de qualification.

Les applications intervenant dans le processus d'authentification et exécutées dans un environnement qui n'est pas de confiance, le cas échéant, doivent avoir fait l'objet d'une qualification par l'Autorité nationale de la sécurité des systèmes d'information attestant de leur conformité au niveau élémentaire, ou supérieur en fonction des risques identifiés, du référentiel général de sécurité.

Chapitre VI
Gestion de la sécurité de l'information

Article 11

La norme ISO 27001 représente une norme réputée et éprouvée en matière de gestion des risques de sécurité de l'information et sa mise en œuvre est recommandée. A défaut de mise en œuvre de cette norme, il convient de démontrer que le système de gestion de la sécurité de l'information adhère à des normes ou des principes apportant un niveau de sécurité similaire.

Chapitre VII
Contrôles techniques

Article 12

Le matériel cryptographique sensible utilisé pour la délivrance des moyens d'identification électronique doit avoir fait l'objet d'une qualification par l'Agence nationale de la sécurité des systèmes d'information attestant de sa conformité au niveau renforcé du référentiel général de sécurité.

Chapitre VIII
Conformité et audits

Article 13

Un programme d'audit doit être mis en place afin de couvrir tous les sujets relatifs à la fourniture des services par l'entité délivrant le moyen d'identification électronique.

Ces audits doivent être effectués avec une fréquence annuelle et l'ensemble du périmètre d'audit doit être couvert tous les trois ans. Ils doivent être assurés par des organismes permettant à l'entité délivrant le moyen d'identification électronique de disposer de garanties sur :

- la compétence et l'indépendance de l'organisme auditeur ainsi que celles de ses auditeurs ;
- la qualité des audits effectués par cet organisme auditeur ;
- la confiance que l'entité auditée peut accorder à l'organisme auditeur en matière de confidentialité avant de leur donner accès à son système et aux informations qu'il contient.