DECRET

Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

NOR: PRMX0909445D

Le Premier ministre,

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la consommation, notamment son article L. 115-28 ;

Vu le code de la défense, notamment son article R.* 1132-3 ;

Vu le code général des collectivités territoriales, notamment son article L. 1211-4-2 ;

Vu la loi n° 2008-776 du 4 août 2008 modifiée de modernisation de l'économie, notamment le I de son article 137 ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment ses articles 9, 10 et 12 ;

Vu le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 97-1184 du 19 décembre 1997 modifié pris pour l'application au Premier ministre du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 97-1194 du 19 décembre 1997 modifié pris pour l'application au ministre de l'économie, des finances et de l'industrie du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

Vu le décret n° 2005-1792 du 30 décembre 2005 portant création d'une direction générale de la modernisation de l'Etat au ministère de l'économie, des finances et de l'industrie ;

Vu le décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie ;

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 la notification à la Commission européenne n° 2008/453/F du 27 octobre 2008 ;

Vu l'avis de la Commission consultative d'évaluation des normes en date du 7 mai 2009 ;

Le Conseil d'Etat (section de l'administration) entendu,

Décrète :

CHAPITRE IER : REFERENTIEL GENERAL DE SECURITE

Article 1

Le référentiel général de sécurité prévu par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

Ces règles sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage, qui permettent de répondre aux objectifs de sécurité mentionnés à l'alinéa précédent.

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité prévu par ce référentiel peut être attestée par une qualification, le cas échéant à un degré donné, régie par le présent décret.

Article 2

· Modifié par Décret n°2012-1221 du 2 novembre 2012 - art. 2 (V)

Le référentiel général de sécurité ainsi que ses mises à jour sont approuvés par arrêté du Premier ministre publié au Journal officiel de la République française. L'Agence nationale de la sécurité des systèmes d'information concourt à l'élaboration de ce référentiel et à sa mise à jour en liaison avec la direction interministérielle pour la modernisation de l'action publique. Ce référentiel est mis à disposition du public par voie électronique.

CHAPITRE II : FONCTIONS DE SECURITE DES SYSTEMES D'INFORMATION

Article 3

Dans les conditions fixées par le référentiel général de sécurité mentionné à l'article 2 du présent décret, l'autorité administrative doit, afin de protéger un système d'information :

1° Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;

2° Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du

système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

3° En déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

Dans les conditions fixées par le référentiel susmentionné, l'autorité administrative réexamine régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

Article 4

Pour mettre en œuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des prestataires de services de confiance ayant fait l'objet d'une qualification dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité.

Article 5

L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.

Dans le cas d'un téléservice, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du téléservice.

CHAPITRE III : QUALIFICATION DES PRODUITS DE SECURITE

Article 6

La demande de qualification d'un produit de sécurité prévue par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée est adressée à l'Agence nationale de la sécurité des systèmes d'information par tout commanditaire, notamment un fabricant ou un fournisseur du produit ou une autorité administrative. La qualification est obtenue à l'issue d'une évaluation des fonctions de sécurité du produit au regard des règles du référentiel général de sécurité.

Article 7

La demande de qualification contient une description du produit et de ses fonctions de sécurité ainsi que les objectifs de sécurité qu'il vise à satisfaire.

L'Agence nationale de la sécurité des systèmes d'information s'assure que le niveau et les

objectifs de sécurité sont cohérents avec le besoin de sécurité des autorités administratives. Elle instruit cette demande lorsque l'ensemble des matériels, des logiciels et de la documentation nécessaires pour réaliser l'évaluation sont disponibles et accessibles.

Article 8

L'évaluation du produit est effectuée dans les conditions et avec les garanties prévues par le décret du 18 avril 2002 susvisé.

Article 9

Le Premier ministre délivre la qualification du produit pour l'un des niveaux fixés par le référentiel, attestant ainsi de sa conformité aux exigences fixées par ce dernier.

Cette attestation est assortie, le cas échéant, de conditions et de réserves et précise sa durée de validité. Elle mentionne les objectifs de sécurité que le produit satisfait et, le cas échéant, le degré de qualification obtenu.

Tout changement des circonstances dans lesquelles la qualification a été délivrée peut conduire le Premier ministre à suspendre ou à retirer la qualification, après que le commanditaire a pu faire valoir ses observations.

CHAPITRE IV : QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE

SECTION 1 : HABILITATION DES ORGANISMES QUI PROCEDENT A LA QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE

Article 10

I. — L'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance prévue par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée est délivrée par le Premier ministre, après vérification :

1° De l'accréditation de l'organisme selon les normes et règles en vigueur, notamment en matière d'impartialité, de responsabilité et de confidentialité. Cette accréditation est délivrée par une instance d'accréditation mentionnée à l'article L. 115-28 du code de la consommation ; et

2° De la compétence technique de l'organisme à conduire l'évaluation de fonctions de sécurité mises en œuvre par un prestataire de services de confiance au regard des règles du référentiel général de sécurité. Cette compétence est appréciée par l'Agence nationale de la sécurité des systèmes d'information à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme.

II. — L'habilitation est valable pour une durée maximale de trois ans renouvelable. Elle

peut énoncer des obligations particulières auxquelles est soumis l'organisme bénéficiaire.

Article 11

· Modifié par Décret n°2011-193 du 21 février 2011 - art. 14
L'Agence nationale de la sécurité des systèmes d'information est informée par l'instance d'accréditation, dans les meilleurs délais, de toute décision d'octroi, de restriction, de refus, de retrait ou de suspension d'accréditation prise dans le cadre des présentes dispositions.

Article 12

La demande d'habilitation prévue à la présente section est adressée à l'Agence nationale de la sécurité des systèmes d'information.

Article 13

L'Agence nationale de la sécurité des systèmes d'information peut s'assurer à tout moment que l'organisme satisfait aux critères et aux obligations fixées par la décision d'habilitation. En cas de manquement, le Premier ministre peut suspendre ou retirer l'habilitation, après qu'un représentant de l'organisme habilité a pu faire valoir ses observations.

Article 14

L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des organismes habilités.

SECTION 2 : QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE PAR DES ORGANISMES HABILITES

Article 15

· Modifié par Décret n°2011-193 du 21 février 2011 - art. 14
Un prestataire de services de confiance peut recevoir une qualification qui atteste de la conformité des services à un niveau de sécurité défini par le référentiel général de sécurité. Il adresse sa demande auprès d'un organisme habilité dans les conditions prévues à la section précédente. L'organisme habilité évalue la conformité des fonctions de sécurité mises en œuvre par le service offert par le prestataire au regard des règles du référentiel général de sécurité correspondant au niveau de sécurité pour lequel la demande de qualification a été faite. L'organisme adresse un rapport d'évaluation à l'Agence nationale de la sécurité des systèmes d'information.

Article 16

Lorsqu'il prononce la qualification, l'organisme habilité délivre à cet effet au prestataire une attestation précisant les fonctions de sécurité couvertes par la qualification et les

conditions s'y attachant. La qualification est valable pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions. L'organisme habilité rend publiques les attestations de qualification qu'il délivre.

Article 17

· Modifié par Décret n°2011-193 du 21 février 2011 - art. 14
Lorsque l'organisme habilité décide de suspendre ou de retirer une qualification ou d'en modifier les conditions, il informe sans délai des raisons à l'origine de ces décisions l'Agence nationale de la sécurité des systèmes d'information. Il rend publique cette décision.

Article 18

Lorsqu'elles recourent à un prestataire de services de confiance qualifié dans les conditions du présent chapitre, les administrations de l'Etat en informent l'Agence nationale de la sécurité des systèmes d'information.

Article 19

Une autorité administrative qui agit comme prestataire de services de confiance pour ses besoins propres ou au profit d'autres autorités administratives peut être qualifiée par un organisme habilité, dans les conditions du présent chapitre.

Lorsque le prestataire de services de confiance est une administration de l'Etat, il doit solliciter au préalable l'avis de l'Agence nationale de la sécurité des systèmes d'information, qui peut proposer de procéder elle-même à l'évaluation des fonctions de sécurité mises en œuvre par cette autorité en vue de sa qualification. Dans ce cas, le Premier ministre délivre la qualification et décide, le cas échéant, de sa suspension ou de son retrait lorsque les conditions s'y attachant ne sont plus satisfaites.

CHAPITRE V : VALIDATION DES CERTIFICATS ELECTRONIQUES

Article 20

Au sens du présent chapitre, on entend par :

1° « Certificat électronique » : des données sous forme électronique attestant du lien entre une autorité administrative ou un agent d'une autorité administrative et des éléments cryptographiques qui lui sont propres et qui sont utilisés par une fonction de sécurité assurant l'identification de cette autorité ou de cet agent dans un système d'information ;

2° « Validation d'un certificat électronique » : la procédure mise en place par l'Etat pour garantir que le certificat électronique d'un agent ou d'une autorité administrative a été délivré par une autorité administrative.

Article 21

En application de l'article 10 de l'ordonnance du 8 décembre 2005 susvisée, l'Agence nationale de la sécurité des systèmes d'information met en place une procédure de validation des certificats électroniques délivrés aux autorités administratives ou à leurs agents.

Article 22

La validation des certificats électroniques d'une autorité administrative ou de ses agents est subordonnée au respect par cette autorité des règles du référentiel général de sécurité relatives à la délivrance de ces certificats. L'Agence nationale de la sécurité des systèmes d'information peut vérifier sur place les conditions de délivrance de ces certificats.

Dans le cas d'un téléservice, les autorités administratives mettent à la disposition de leurs usagers les informations, dont la liste est fixée par un arrêté du Premier ministre, relatives à la délivrance et à la validation de leurs certificats électroniques.

Article 23

Un arrêté du Premier ministre précise les modalités de mise en œuvre de la procédure de validation. Les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans les trois ans à compter de la publication de cet arrêté.

CHAPITRE VI : REFERENCEMENT DES PRODUITS DE SECURITE ET DES PRESTATAIRES DE SERVICES DE CONFIANCE

Article 24

Le référencement d'un produit de sécurité ou d'un prestataire de services de confiance mentionné à l'article 12 de l'ordonnance du 8 décembre 2005 susvisée est subordonné au respect des prescriptions contenues dans un cahier des charges approuvé par arrêté du ministre chargé de la réforme de l'Etat. Ce cahier des charges détermine notamment les conditions dans lesquelles l'interopérabilité des produits de sécurité et des prestataires de services de confiance qualifiés dans les conditions prévues au présent décret est vérifiée ainsi que les tests qui sont réalisés à cette fin.

Le référencement mentionné au premier alinéa est prononcé par décision du ministre chargé de la réforme de l'Etat.

CHAPITRE VII : DISPOSITIONS DIVERSES

Article 25

A modifié les dispositions suivantes :
- Modifie Décret n°2002-535 du 18 avril 2002 - art. 11 (V)

Article 26

· Modifié par Décret n°2012-1221 du 2 novembre 2012 - art. 2 (V)
A modifié les dispositions suivantes :

-Décret n° 97-1184 du 19 décembre 1997

Art. ANNEXE

-Décret n° 97-1194 du 19 décembre 1997

Art. Annexe

II.-Au 2 du titre II de l'annexe au décret n° 97-1194 du 19 décembre 1997 susvisé, il est ajouté à la suite du tableau relatif aux décisions entrant dans le champ de compétences de la direction générale des douanes et droits indirects les mots et le tableau suivants :
Décisions entrant dans le champ de compétences de la direction interministérielle pour la modernisation de l'action publique.
Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives :

1	Référencement des produits de sécurité et des prestataires de services de confiance.	Second alinéa de l'article 24.

Article 27

A modifié les dispositions suivantes :
· Modifie Décret n°2009-834 du 7 juillet 2009 - art. 4 (V)

Article 28

Les dispositions du présent décret peuvent être modifiées par décret, à l'exception des articles 1er, 2, 9, du premier alinéa de l'article 10, de l'article 13, du second alinéa de l'article 19, du second alinéa de l'article 24 et de l'article 26.

Article 29

La ministre de l'économie, de l'industrie et de l'emploi et le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'Etat sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 2 février 2010.

François Fillon

Par le Premier ministre :

La ministre de l’économie,
de l’industrie et de l’emploi,
Christine Lagarde
Le ministre du budget, des comptes publics,
de la fonction publique
et de la réforme de l’Etat,
Eric Woerth