DECRET

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

NOR: PRMX0100183D

Version consolidée au 9 octobre 2012

Le Président de la République,

Sur le rapport du Premier ministre, du ministre de l'économie, des finances et de l'industrie et du ministre délégué à l'industrie, aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation,

Vu la directive 98/34/CE du 22 juin 1998, modifiée par la directive 98/48/CE du 20 juillet 1998, 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 R. 115-6 ;

Vu le décret n° 97-34 du 15 janvier 1997, modifié par le décret n° 97-463 du 9 mai 1997 et par le décret n° 97-1205 du 19 décembre 1997, relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 97-1184 du 19 décembre 1997, modifié par le décret n° 2001-143 du 15 février 2001, 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° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Le Conseil d'Etat (section de l'intérieur) entendu ;

Le conseil des ministres entendu,

Article 1

La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance peut être certifiée dans les conditions prévues au présent décret.

Les administrations de l'Etat recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret.

Chapitre Ier : Procédure d'évaluation et de certification

Section 1 : Evaluation.

Article 2

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à l'Agence nationale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.
Dès réception de ce dossier, l'Agence nationale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

Article 3

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
Le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation, agréés dans les conditions prévues au chapitre II, pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres :

a) Le produit ou le système à évaluer ainsi que les objectifs de sécurité ;
b) Les conditions de protection de la confidentialité des informations qui seront traitées dans le cadre de l'évaluation ;
c) Le coût et les modalités de paiement de l'évaluation ;
d) Le programme de travail et les délais prévus pour l'évaluation.

Le commanditaire est tenu d'assurer la mise à la disposition des centres d'évaluation qu'il a choisis et de l'Agence nationale de la sécurité des systèmes d'information, si elle en fait la demande, de tous les éléments nécessaires au bon accomplissement de leurs travaux, le cas échéant après accord des fabricants concernés.

Article 4

Le commanditaire peut décider à tout moment de mettre fin à une évaluation.

Il est décidé entre les parties du dédommagement éventuellement dû au centre d'évaluation.

Article 5

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
L'Agence nationale de la sécurité des systèmes d'information veille à la bonne exécution des travaux d'évaluation. Elle peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement.

Article 6

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
Au terme des travaux d'évaluation, chaque centre remet un rapport d'évaluation au commanditaire et à l'Agence nationale de la sécurité des systèmes d'information. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial.

Section 2 : Certification.

Article 7

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
Le commanditaire et l'Agence nationale de la sécurité des systèmes d'information valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Lorsque l'ensemble des rapports prévus a été validé, l'Agence nationale de la sécurité des systèmes d'information élabore un rapport de certification dans un délai d'un mois. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification.
Le rapport de certification peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Il est, au choix du commanditaire, communiqué ou non à des tiers ou rendu public.

Article 8

Le certificat est délivré par le Premier ministre.

Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

Article 9

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
L'Agence nationale de la sécurité des systèmes d'information peut passer, après avis du comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues, ayant leur siège en dehors des Etats membres de la Communauté européenne.
Ces accords peuvent prévoir que les certificats délivrés par les organismes étrangers cosignataires, dans le cadre de procédures comparables à celle prévue au présent chapitre, sont reconnus comme ayant la même valeur que les certificats délivrés en application du présent décret. La reconnaissance mutuelle des certificats peut être limitée à un niveau d'assurance déterminé.
Sans préjudice des règles régissant la certification des dispositifs sécurisés de création de signature électronique mentionnées au 2° du II de l'article 3 du décret du 30 mars 2001 susvisé, le Premier ministre reconnaît aux certificats délivrés par les organismes ayant leur siège dans un Etat membre de la Communauté européenne, dans le cadre de procédures comparables présentant des garanties équivalentes, la même valeur qu'aux certificats délivrés en application du présent décret.

Chapitre II : Agrément des centres d'évaluation.

Article 10

Modifié par Décret n°2010-1630 du 23 décembre 2010 - art. 2

Les centres d'évaluation chargés de procéder à l'évaluation prévue au présent décret et aux articles R. 331-85 à R. 331-88 du code de la propriété intellectuelle sont agréés dans les conditions fixées par le présent chapitre.

Article 11

Modifié par Décret n°2010-112 du 2 février 2010 - art. 25
I.-La demande d'agrément est formulée auprès de l'Agence nationale de la sécurité des systèmes d'information. Cette demande précise le domaine dans lequel l'organisme demandeur entend exercer son activité.

II.-L'organisme demandeur doit faire la preuve :

a) De sa conformité à des critères de qualité selon les règles ou les normes en vigueur ;
b) De son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante ainsi qu'à assurer la confidentialité requise par l'évaluation ;
c) De sa compétence technique à conduire une évaluation.

La conformité mentionnée au a et l'aptitude mentionnée au b sont attestées soit par une accréditation délivrée par une instance d'accréditation mentionnée à l'article L. 115-28 du code de la consommation, soit par l'Agence nationale de la sécurité des systèmes d'information.
La compétence technique mentionnée au c est appréciée par l'Agence nationale de la

sécurité des systèmes d'information, notamment à partir des moyens, des ressources et de l'expérience du centre d'évaluation.

Article 12

L'agrément est délivré par le Premier ministre, après avis du comité directeur de la certification.

Il peut énoncer les obligations particulières auxquelles est soumis le centre d'évaluation.

Il est valable pour une durée de deux ans renouvelable.

Article 13

Lorsqu'un centre d'évaluation situé hors du territoire national ou d'un autre Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de son pays d'installation dans le cadre d'une procédure homologue, le Premier ministre peut, après avis du comité directeur de la certification, le déclarer agréé au titre du présent décret. Cet agrément, qui est accordé pour une durée de deux ans renouvelable, peut être limité à un niveau d'assurance déterminé.

Lorsqu'un centre d'évaluation situé dans un Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de cet Etat dans le cadre d'une procédure équivalente, le Premier ministre, après avis du comité directeur de la certification, le déclare agréé au titre du présent décret.

Article 14

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
L'Agence nationale de la sécurité des systèmes d'information peut s'assurer à tout moment que les centres d'évaluation continuent à satisfaire aux critères au vu desquels ils ont été agréés.
Lorsqu'un centre ne satisfait plus aux exigences mentionnées à l'article 11 ou qu'il manque aux obligations fixées par la décision d'agrément, l'agrément peut être retiré par le Premier ministre, après avis du comité directeur de la certification. Le retrait ne peut être prononcé qu'après que le représentant du centre d'évaluation a été mis à même de faire valoir ses observations devant le comité directeur de la certification.

Chapitre III : Comité directeur de la certification en sécurité des technologies de l'information.

Article 15

Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :

a) De formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et

sur les guides techniques mis à la disposition du public ;

b) D'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;

c) D'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;

d) D'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.

La mission prévue au c ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

Article 16

Le comité directeur de la certification en sécurité des technologies de l'information est présidé par le secrétaire général de la défense et de la sécurité nationale ou son représentant. Outre son président, il comprend :

a) Un représentant du ministre de la justice ;
b) Un représentant du ministre de l'intérieur ;
c) Un représentant du ministre des affaires étrangères ;
d) Un représentant du ministre de la défense ;
e) Un représentant du ministre chargé de l'industrie ;
f) Un représentant du ministre chargé de l'économie ;
g) Un représentant du ministre chargé de l'emploi ;
h) Un représentant du ministre chargé de la santé ;
i) Un représentant du ministre chargé de l'éducation nationale ;
j) Un représentant du ministre chargé de la communication ;
k) Un représentant du ministre chargé de la réforme de l'Etat ;
l) Un représentant du ministre chargé des transports ;
m) Un représentant du ministre chargé de la recherche.

Lorsque le comité directeur examine des questions concernant les dispositifs de création et de vérification de signature électronique, tels que définis à l'article 1er du décret du 30 mars 2001 susvisé, il comprend en outre douze personnalités qualifiées nommées pour trois ans par arrêté du Premier ministre.
Le secrétariat du comité directeur est assuré par l'Agence nationale de la sécurité des systèmes d'information.

Article 17

Le comité directeur se réunit sur convocation de son président qui en fixe l'ordre du jour.

Le président peut inviter tout expert ou personne qualifiée dont la participation aux débats lui paraît nécessaire.

Le comité rend compte de ses travaux au Premier ministre.

Article 18

Modifié par Décret n°2009-834 du 7 juillet 2009 - art. 9 (V)
L'Agence nationale de la sécurité des systèmes d'information fait annuellement rapport au comité directeur de la certification de l'activité qu'elle exerce dans le cadre de la mise en oeuvre du présent décret.

Article 19

A modifié les dispositions suivantes :
Modifie Décret n°97-1184 du 19 décembre 1997 - art. ANNEXE (M)

Article 20

A modifié les dispositions suivantes :
Modifie Décret n°2001-272 du 30 mars 2001 - art. 3 (V)
Modifie Décret n°2001-272 du 30 mars 2001 - art. 4 (V)
Modifie Décret n°2001-272 du 30 mars 2001 - art. 5 (V)
Modifie Décret n°2001-272 du 30 mars 2001 - art. 7 (V)
Modifie Décret n°2001-272 du 30 mars 2001 - art. 9 (M)

Chapitre IV : Dispositions diverses et transitoires.

Article 21

Les certificats et les agréments des centres d'évaluation délivrés avant la date d'entrée en vigueur du présent décret, en application des dispositions de l'avis du Premier ministre relatif à la délivrance de certificats pour la sécurité offerte par les produits informatiques vis-à-vis de la malveillance, publié au Journal officiel de la République française du 1er septembre 1995, sont reconnus comme délivrés au titre du présent décret.

Article 22

Le présent décret est applicable :

a) En Nouvelle-Calédonie et en Polynésie française, en tant qu'il concerne la signature électronique ;
b) Dans les îles Wallis et Futuna et à Mayotte.

Article 23

Les dispositions du présent décret pourront être ultérieurement modifiées par décret, à l'exception :

a) Du premier alinéa des articles 8 et 12, du deuxième alinéa de l'article 14 et de l'article 19 dont la modification s'effectuera, le cas échéant, dans les conditions prévues à l'article 2 du décret du 15 janvier 1997 susvisé ;

b) De l’article 20.

Article 24

Le présent décret sera publié au Journal officiel de la République française.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,

Lionel Jospin

Le ministre de l’économie,

des finances et de l’industrie,

Laurent Fabius

La garde des sceaux, ministre de la justice,

Marylise Lebranchu

Le ministre de l’intérieur,

Daniel Vaillant

Le ministre délégué à l’industrie,

aux petites et moyennes entreprises,

au commerce, à l’artisanat

et à la consommation,

Christian Pierret

Le secrétaire d’Etat à l’outre-mer,

Christian Paul