PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 8 avril 2011

N° 1001/ANSSI/SR

NOR :	PRM	D	1	2	0	1	2	9	7	C

Instruction

relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance

Version 1.0

Cette instruction est prise en application de l'article 10 du décret n° 2010-112 du 2 février 2010 pris pour 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.

Cette instruction s'applique aux prestataires de services de confiance décrits dans le référentiel général de sécurité en version 1.0 approuvée par arrêté du Premier ministre le 6 mai 2010.

Le directeur général
de l'Agence nationale de la sécurité
des systèmes d'information

Patrick PAILLOUX

[ORIGINAL SIGNE]

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**
08/04/2011	1.0	*Publication de l'instruction*

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information
SGDSN/ANSSI
Bureau de la Réglementation
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP
rgs [at] ssi.gouv.fr

La présente instruction est disponible en ligne sur les sites suivants :

- le site institutionnel de l'ANSSI (www.ssi.gouv.fr) ;
- le site institutionnel du SGDSN (www.sgdsn.gouv.fr) ;
- le site du Premier ministre dédié à la publication des instructions et circulaires (www.circulaires.gouv.fr).

Sommaire

1. Objet de l'instruction 4
2. Références 4
3. Demande d'habilitation 5
4. Examen du dossier de demande d'habilitation 6
5. Audit de l'organisme candidat 6
6. Décision d'habilitation 6
7. Suivi de l'habilitation 7
8. Modification de la portée de l'habilitation 7
9. Arrivée, départ et évolution des compétences et des responsabilités des auditeurs 7
10. Renouvellement de l'habilitation 7
11. Suspension et retrait de l'habilitation 8
Annexe 1 : Lettre de demande type 9
Annexe 2 : Portée de l'habilitation 11

1. Objet de l'instruction

La présente instruction définit la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance prévue par l'article 9 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.

Conformément à l'article 10 du décret n° 2010-112 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005, la procédure d'habilitation d'un organisme candidat vise à s'assurer de :

a. la conformité de l'organisme aux critères de qualité et de technicité selon les règles et normes d'accréditation en vigueur, notamment en matière d'impartialité, de responsabilité, de confidentialité et de compétence. Cette conformité est vérifiée par le Comité français d'accréditation (COFRAC), qui prononce l'accréditation de l'organisme candidat ;
b. la compétence technique de l'organisme à conduire l'évaluation de fonctions de sécurité mises en œuvre par un prestataire de services de confiance (PSCO) au regard des règles du référentiel général de sécurité (RGS). Cette conformité est vérifiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

L'habilitation est délivrée par l'ANSSI au nom du Premier ministre.

2. Références

[Ordonnance]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Voir www.legifrance.gouv.fr
[DécretRGS]	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. . Voir www.legifrance.gouv.fr
[RGS]	Référentiel général de sécurité, version 1.0 approuvée par arrêté du Premier ministre le 6 mai 2010. www.ssi.gouv.fr/rgs
[ISO-17021]	Evaluation de la conformité : Exigences pour les organismes procédant à l'audit et à la certification de systèmes de management, version du 15 septembre 2006. Disponible (payant) sur le site de l'Association française de normalisation (AFNOR) : www.afnor.org.
[ISO-19011]	Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental, version du 1er octobre 2002. Disponible (payant) sur le site de l'Association française de normalisation (AFNOR) : www.afnor.org.
[CEPE-REF-21]	Exigences spécifiques pour la qualification des prestataires de services de confiance. www.cofrac.fr/documentation/CEPE-REF-21

3. Demande d’habilitation

La demande d’habilitation est constituée d’une lettre et d’un dossier. Conformément à l’article 12 du [DécretRGS], elle est adressée à l’ANSSI. Cette demande est envoyée au format papier à l’adresse ci-dessous et peut être accompagnée d’un support physique (CD-ROM, clé USB…) contenant le dossier de demande au format électronique.

Agence nationale de la sécurité des systèmes d’information
SGDSN/ANSSI
Bureau de la Réglementation
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

La lettre de demande est signée par le représentant légal de l’organisme candidat, qui prend les engagements mentionnés dans la lettre de demande type fournie en annexe 1.

Elle précise la portée de l’habilitation demandée, selon les formes précisées en annexe 2.

Le dossier de demande d’habilitation doit comporter :

a. un extrait K-BIS original de la société dont dépend l’organisme candidat datant de moins de deux mois ;
b. une photocopie de l’attestation d’accréditation délivrée par le COFRAC[1], incluant la portée ;
c. les éléments permettant d’apprécier les capacités de l’organisme candidat, comprenant :
    - une présentation générale de l’organisme précisant notamment ses moyens, ses ressources, son expérience, ainsi que les organigrammes présentant les différentes responsabilités ;
    - une présentation des activités de l’organisme et, le cas échéant, des prestations d’audit similaires (coordonnées des responsables chez les clients, rapports d’audit…) ;
d. les éléments permettant d’apprécier les compétences techniques du personnel qui réalisera les audits de PSCO pour le compte de l’organisme candidat (ci-après désignés « auditeurs ») :
    - une photocopie d’une pièce d’identité en cours de validité ;
    - le *curriculum vitae* de l’auditeur, précisant notamment ses diplômes, les formations à la sécurité des systèmes d’information et à l’audit qu’il a suivies, ainsi que l’expérience acquise ;
    - le domaine technique[2] pour lequel l’auditeur exercera sa fonction, ainsi que tout élément permettant d’apprécier l’expertise et l’expérience de l’auditeur dans ce domaine ;
    - le type de contrat qui le lie à l’organisme candidat ;
    - un engagement de l’auditeur garantissant son impartialité, son indépendance par rapport aux acteurs économiques du domaine technique qu’il couvre et le respect de la confidentialité des prestations d’audit ;

[1] Cette accréditation est délivrée sur la base de la vérification de la conformité de l’organisme candidat avec la norme [ISO-17021] complétée des exigences spécifiques liées à la qualification des PSCO décrites dans le document [CEPE-REF-21].

[2] Le domaine technique couvert par un auditeur désigne les familles de PSCO, les usages et les niveaux de sécurité pour lesquels l’auditeur sera amené à réaliser des audits.

e. les mesures de sécurité des locaux et des systèmes d’information de l’organisme candidat ;
f. tout autre élément pouvant apporter des informations utiles sur l’organisme candidat ou les auditeurs.

4. Examen du dossier de demande d’habilitation

L’ANSSI accuse réception de la demande d’habilitation et désigne une personne en charge du traitement de la demande. Elle peut requérir, le cas échéant, la fourniture de pièces complémentaires.

5. Audit de l’organisme candidat

Afin de s’assurer de la capacité de l’organisme candidat à conduire l’évaluation, au regard des règles du RGS, de fonctions de sécurité mises en œuvre par un PSCO, l’ANSSI analyse et vérifie en particulier :

a. les éléments fournis dans le dossier de demande ;
b. la compétence technique de chaque auditeur dans le domaine de la sécurité des systèmes d’information (son expérience, sa connaissance du RGS, le suivi dans le temps de ses compétences) ;
c. l’adéquation des compétences de l’ensemble des auditeurs au regard de la portée d’habilitation demandée par l’organisme candidat ;
d. les procédures permettant de garantir :
    - le maintien dans le temps des compétences des auditeurs ;
    - l’impartialité et l’indépendance des auditeurs ;
    - le respect des règles de confidentialité par les auditeurs ;
e. les mesures de sécurité des locaux et des systèmes d’information de l’organisme candidat.

A cet effet, l’ANSSI peut procéder à des entretiens avec toute personne membre de l’organisme candidat et les auditeurs. Elle peut se rendre dans les locaux de l’organisme candidat ou accompagner un auditeur lors d’un audit de PSCO, avec l’accord de ce PSCO.

L’ANSSI s’assure de l’impartialité des agents qui procèdent à l’audit de l’organisme candidat.

6. Décision d’habilitation

La décision d’habilitation est prononcée par le directeur général de l’ANSSI par délégation du Premier ministre et notifiée à l’organisme candidat. Elle indique la portée de l’habilitation, qui peut être réduite par rapport à la portée initialement demandée par l’organisme candidat, et précise la durée de validité de l’habilitation. Une copie de la décision est adressée au COFRAC.

Conformément à l’article 10.II du [DécretRGS], cette décision peut énoncer des obligations particulières auxquelles est soumis l’organisme habilité (ci-après désignés « organisme de qualification ») ; et, dans ce cas, fixer le délai de mise en œuvre des obligations

En complément, l’ANSSI envoie à l'organisme de qualification la liste des auditeurs aptes à participer aux qualifications de PSCO, et pour chacun, le domaine technique pour lequel il a été reconnu compétent (cette liste est ci-après désignée « liste des auditeurs compétents »).

L’ANSSI met en ligne sur son site Internet la liste des organismes de qualification ainsi que la portée de leur habilitation, conformément à l’article 14 du [DécretRGS].

7. Suivi de l’habilitation

Conformément à l’article 13 du [DécretRGS], l’ANSSI peut s’assurer à tout moment que l’organisme de qualification continue de satisfaire aux critères d’habilitation, en procédant à tout ou partie de l’audit prévu au paragraphe 5.

8. Modification de la portée de l’habilitation

L’organisme de qualification peut demander à l’ANSSI une modification de la portée de son habilitation, dans les limites de la portée inscrite dans son attestation d’accréditation, dans le cas notamment où il s’est attaché les services d’auditeurs experts dans un nouveau domaine. Il transmet à l’ANSSI l’ensemble des éléments qui justifient sa demande.

L’ANSSI instruit la demande et, le cas échéant, décide de la modification de la portée d’habilitation et met à jour la liste des auditeurs compétents. Elle adresse la décision d’habilitation et la liste des auditeurs compétents à l’organisme de qualification ainsi qu’une copie de la décision au COFRAC

L’ANSSI peut décider de la réduction de la portée de l’habilitation de l’organisme de qualification, notamment quand les compétences de l’organisme ne couvrent plus la portée initialement accordée (départ d’experts par exemple). Elle informe de son intention l’organisme de qualification et lui en fournit les motifs. L’organisme de qualification dispose de quinze jours pour faire valoir ses observations.

9. Arrivée, départ et évolution des compétences et des responsabilités des auditeurs

L’organisme de qualification informe l’ANSSI de toute arrivée, départ ou évolution des compétences et des responsabilités d’un auditeur.

9.1. Arrivée d’un auditeur

L’organisme de qualification transmet à l’ANSSI le dossier permettant d’apprécier les compétences techniques de l’auditeur (cf. paragraphe 3 d. et e.).

Lorsque l'ANSSI reconnaît la compétence de l’auditeur, elle adresse à l’organisme de qualification la liste des auditeurs compétents mise à jour.

9.2. Départ d’un auditeur

L’ANSSI instruit éventuellement la réduction de la portée de l’habilitation qui fait suite au départ de l’auditeur (cf. paragraphe 8).

9.3. Évolution des compétences d’un auditeur

L’organisme de qualification transmet à l’ANSSI le dossier permettant d’apprécier l’évolution des compétences techniques de l’auditeur (cf. paragraphe 3 d. et e.).

Lorsque l'ANSSI reconnaît l’évolution des compétences de l’auditeur, elle adresse à l’organisme de qualification la liste des personnels compétents mise à jour.

Lorsque l'ANSSI reconnaît la compétence de l’auditeur, elle adresse à l’organisme de qualification la liste des personnels compétents mise à jour.

10. Renouvellement de l’habilitation

Trois mois avant l’échéance de la validité de l’habilitation, l’organisme de qualification doit demander à l’ANSSI, s’il le souhaite, le renouvellement de son habilitation.

A la réception de la demande de renouvellement, l'ANSSI réalise un nouvel audit de l'organisme de qualification. Si les critères d'habilitation sont toujours respectés, une nouvelle décision d'habilitation est prononcée par le directeur général de l'ANSSI.

A défaut, à l'échéance, l'organisme de qualification est retiré de la liste des organismes habilités publiée par l'ANSSI.

11. <u>Suspension et retrait de l'habilitation</u>

Conformément à l'article 13 du [décret RGS], tout ou partie de la portée de l'habilitation de l'organisme de qualification peut être suspendue ou retirée, après qu'un représentant de l'organisme de qualification ait pu faire valoir ses observations.

Lorsque l'ANSSI envisage de suspendre ou de retirer une habilitation, elle en informe l'organisme de qualification et lui en fournit les motifs. L'organisme de qualification dispose de quinze jours pour faire valoir ses observations.

A l'issue de ce délai, en fonction de la réponse de l'organisme de qualification, l'ANSSI peut maintenir, suspendre ou retirer l'habilitation.

Les causes de suspension ou de retrait d'habilitation sont notamment :

- l'échéance ou le retrait de l'accréditation délivrée par le COFRAC pour les activités de qualification de PSCO ;
- un changement majeur dans l'organisation de l'organisme, ou dans la société dont il dépend (statuts, actionnariat, dirigeants, procédures collectives…), remettant en cause les critères sur lesquels l'organisme de qualification a été habilité ;
- le non-respect des obligations fixées par la décision d'habilitation ;
- le non-respect des engagements pris lors du dépôt de sa demande d'habilitation ;
- le départ de l'ensemble des responsables d'audit ;
- la cessation totale ou partielle de l'activité de l'organisme de qualification.

Annexe 1 :

Lettre de demande type

Demande d’habilitation

A rédiger sur le papier à en-tête de l’organisme candidat,
et à adresser à :

Agence nationale de la sécurité des systèmes d’information SGDSN/ANSSI Bureau de la réglementation 51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP FRANCE

Je soussigné, **[mandataire social de la société ou nom de la personne autorisée à engager la société], [titre]** de la société **[société],** demande l’habilitation de l’organisme **[nom de l’organisme candidat]** en vue de procéder à la qualification des prestataires de services de confiance prévue par l’article 9 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.

A ce jour, **[Nom de la Société]** est une société ayant une existence valide et légale dont le siège est **[Ville]**.

Je demande cette habilitation avec la portée suivante :

a. **[familles de PSCO] ;**
b. **[prestations de services de confiance] ;**
c. **[niveaux de sécurité de chaque prestation].**

Je vous adresse ci-joint le dossier correspondant à ma demande et certifie que les informations qu’il contient sont exactes.

Je m’engage à :

- rendre compte à l’ANSSI de toute évolution substantielle des informations fournies dans le dossier de demande d’habilitation et, notamment, celles relatives à la structure de l’organisme, son organisation et au personnel chargé des audits ;
- assurer à l’ANSSI l’accès à ses locaux, à l’ensemble des documents utilisés dans le cadre de la qualification des prestataires de services de confiance, à son personnel et à ses auditeurs ;

- autoriser l'ANSSI à assister à tout moment au déroulement d'une évaluation d'un prestataire de services de confiance, dans les locaux de l'organisme de qualification ou directement chez le prestataire ;
- communiquer à l'ANSSI, à chaque évolution, la liste des prestataires de services de confiance qualifiés ;
- informer l'ANSSI, dès réception du dossier, des demandes de qualification (incluant les noms, coordonnées, activités et portée souhaitée de la qualification des prestataires de services) ;
- ne recourir qu'aux auditeurs reconnus compétents par l'ANSSI pour procéder à la qualification des prestataires de services de confiance ;
- garantir la complémentarité des compétences des auditeurs lors d'une qualification ;

Conformément aux articles 15 et 17 du décret n° 2010-112 du 2 février 2010, je suis tenu de communiquer à l'ANSSI, sans délai :

- les rapports d'évaluation des prestataires de services de confiance ayant effectué une demande de qualification, quelle qu'en soit l'issue ;
- toute décision de suspension, de retrait ou de modification des conditions d'une qualification.

Le point de contact pour le suivi de la procédure d'habilitation est **[nom], [titre], [téléphone], [courriel], [adresse]**.

[Date]

[Signature]

Annexe 2 :

Portée de l'habilitation

La portée de l'habilitation décrit les prestations de services de confiance pour lesquelles l'organisme de qualification est habilité à réaliser des audits et à prononcer des qualifications.

Elle précise :

- le type de famille de PSCO ;
- les prestations de services de confiance ;
- le cas échéant, le niveau de sécurité de chaque prestation.

La première version du [RGS] contient des règles permettant de qualifier deux familles de PSCO :

- les prestataires de services de certification électronique (PSCE). Ces prestataires peuvent délivrer des certificats électroniques pour des usages tels que la signature électronique, l'authentification, le chiffrement et ce pour trois niveaux de sécurité (*), (**) et (***) ;
- les prestataires de services d'horodatage électronique (PSHE). Ces prestataires délivrent des contremarques de temps pour un unique niveau de sécurité.

Les portées correspondantes sont :

Famille de PSCO	Prestations de services de confiance	Niveaux de sécurité
PSCE	Certificats électroniques de chiffrement	*, **, ***
PSCE	Certificats électroniques d'authentification	*, **, ***
PSCE	Certificats électroniques de signature électronique	*, **, ***
PSCE	Certificats électroniques d'authentification serveur	*, **, ***
PSCE	Certificats électroniques de cachet	*, **, ***
PSCE	Certificats électroniques d'authentification et de signature	*, **
PSHE	Horodatage	un seul niveau