Exigences spécifiques pour l'accréditation des organismes procédant à la certification des prestations liées à la sécurité des systèmes d'information

CERT CPS REF 33 - Révision 04

SOMMAIRE

1. OBJET

Ce document définit les exigences à satisfaire et le processus d'accréditation pour l'évaluation et la certification des prestations liées à la sécurité des systèmes d'information selon

- Le référentiel PASSI
- Le RGS
- Le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS »
- Le référentiel SecNumCloud

2. REFERENCES ET DEFINITIONS

2.1. Références

Ce document s'applique en complément des documents référencés ci-dessous.

2.1.1 Publications de l'ISO

- NF EN ISO/CEI 17065 : Exigences pour les organismes certifiant les produits, les procédés et les services

2.1.2 Autres textes de référence

2.1.2.1 Pour les PASSI

Textes règlementaires

- 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,
- Décret n°2015-350 du 27 mars 2015, relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

Ces documents sont disponibles sur www.legifrance.fr.

Textes de l'ANSSI

- Prestataires d'audit de la sécurité des systèmes d'information — référentiel d'exigences, document dénommé [PASSI], version en vigueur,
- Référentiel d'exigences applicables aux prestataires d'audit et de contrôle de la sécurité des systèmes d'information pour les besoins de la sécurité nationale, document dénommé [PASSI_LPM], version en vigueur. Ce document n'est pas public, mais est communiqué par l'ANSSI aux candidats à la qualification sous réserve qu'ils disposent des moyens de protéger cette information,
- Processus de qualification d'un service, document dénommé [QUAL_SERV_PROCESS] version en vigueur,
- Portée de qualification des services, document dénommé [QUAL_SERV_PORTEES],
- Exigences applicables aux centres d'évaluation de services, document dénommé [QUAL_SERV_CE], version en vigueur. Dans l'attente de la publication de ce document aucune exigence spécifique nouvelle ne s'applique aux centres d'évaluation de services,

- Trame d'évaluation des prestataires d'audit de la sécurité des systèmes d'information [TRAME_PASSI], version en vigueur. Ce document est mis à disposition des organismes de certification candidats par l'ANSSI,
- Référentiel général de sécurité, version en vigueur. Ce document est dénommé [RGS].

Ces documents sont ou seront disponibles sur www.ssi.gouv.fr ou communiqués par l'ANSSI sur demande. L'organisme de certification est informé par l'ANSSI des mises à jour de ces documents et des modalités de transition.

2.1.2.2 Pour les PSCE et PSHE entrant dans le champ d'application du décret n°2010-112 du 2 février 2010

Textes règlementaires

- 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,

Ce document est disponible sur www.legifrance.fr .

Textes de l'ANSSI

- [QUAL_SERV_PROCESS],
- [QUAL_SERV_CE],
- [RGS].

Ces documents sont ou seront disponibles sur www.ssi.gouv.fr ou communiqués par l'ANSSI sur demande. L'organisme de certification est informé par l'ANSSI des mises à jour de ces documents et des modalités de transition.

2.1.2.3 Pour les PSCo entrant dans le champ d'application du Règlement (UE) n°910/2014 (eIDAS)

- Règlement (UE) n°910/2014 du 23/07/2014 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, (dit règlement eIDAS),
- ETSI EN 319 403, Electronic Signatures and Infrastructures; Trust Service Provider Conformity Assessment – Requirements for conformity assessments bodies assessing Trust Services Providers.

Exigences pour les certifiés :

- ETSI EN 319 401, Electronic Signatures and Infrastructures ; General Policy Requirements for Trust Service Providers,
- ETSI EN 319 411, Electronic Signatures and Infrastructures ; Policy and security requirements for trust Service Providers issuing certificates; Part 1 et Part 2 (prestations de services de signature électronique),
- ETSI EN 319 421, Electronic Signatures and Infrastructures; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, (prestations de services d'horodatage électronique),

- ETSI EN 319 102-1, Electronic Signatures and Infrastructures (ESI); Procedures for creation and validation of ades digital signatures ; part 1 : creation and validation (prestation de services de validation des signatures électroniques et des cachets électroniques)
- ETSI TS 102 640-3, Electronic Signatures and Infrastructures; registered electronic mail – Part 3: information security policy requirements for REM domains. (prestations de services d'envoi recommandé électronique)

Et tous documents émanant de l'European Telecommunication Standard Institute (ETSI) référencés dans ces documents et/ou publiés sur le site www.etsi.org/standards/search

Dans le cadre d'une certification au titre du règlement eIDAS, l'Organisme de Certification devra se rapprocher de l'organe de contrôle de chaque État Membre dans lequel il souhaite certifier des Prestataires de Service de Confiance (PSCo) afin d'obtenir la liste des exigences applicables pour chaque service de confiance, si celles-ci ont été définies.

Au niveau national

Selon le pays dans lequel le prestataire demande sa certification, les modalités de respect des exigences du règlement eIDAS peuvent être précisées au niveau national par l'organe de contrôle désigné pour ce pays.

Pour la France, les exigences applicables sont précisées dans les documents suivants, publiés sur le site ssi.gouv.fr, en fonction de la nature du service de confiance concerné, et de sa qualification préalable selon le RGS ou non :

- Prestataires de services de confiance qualifiés – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services de validation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services de conservation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services d'envoi recommandé électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – version en vigueur,
- Services d'horodatage électronique qualifiés – modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS – version en vigueur,
- Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS – version en vigueur,
- Document de l'ANSSI [CRITERES_OEC] : Organismes d'évaluation de la conformité des prestataires de service de confiance – Critères de reconnaissance au titre du règlement eIDAS.

L'organisme de certification est informé par l'ANSSI des mises à jour de ces documents et des modalités de transition.

2.1.2.4 Pour les prestataires de services d'informatique en nuage (SecNumCloud)

Textes de l'ANSSI

- Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences
- [QUAL_SERV_PROCESS],
- [QUAL_SERV_PORTEES],
- [QUAL_SERV_CE],
- Note de l'ANSSI n°17220/ANSSI/SDE/BQA du 22 octobre 2018 ayant pour objet la Trame d'évaluation des prestataires de service d'informatique en nuage (SecNumCloud).

Ces documents sont ou seront disponibles sur www.ssi.gouv.fr ou communiqués par l'ANSSI sur demande. L'organisme de certification est informé par l'ANSSI des mises à jour de ces documents et des modalités de transition.

2.2. Abréviations et définitions

Les abréviations suivantes sont utilisées dans la suite de ce document :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
COFRAC	Comité Français d'Accréditation
ETSI	European Telecommunication Standard Institute
OC	Organisme de Certification
RGS	Référentiel général de sécurité
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
PSCo	Prestataire de Service de Confiance
PSCE	Prestataire de Service de Certification Electronique
PSHE	Prestataire de Service d'Horodatage Electronique

3. DOMAINE D'APPLICATION

Ce document s'applique à toutes les demandes d'accréditation et aux organismes accrédités pour :

- Les qualifications des prestations d'audit de la sécurité des systèmes d'information (PASSI) entrant dans le champ d'application du Référentiel général de sécurité (RGS) au titre du décret n°2010-112 du 2 février 2010
- Les qualifications des prestations d'audit de la sécurité des systèmes d'information (PASSI) pour les besoins de la sécurité des systèmes d'information au titre du décret n°2015-350 du 27 mars 2015

qui s'inscrivent dans le cadre de l'application des documents référencés au §2.1.2.1 ;

- Les qualifications des prestataires de service de certification électronique (PSCE) entrant dans le champ d'application du Référentiel général de sécurité (RGS) au titre du décret n°2010-112 du 2 février 2010
- Les qualifications des prestataires de service d'horodatage électronique (PSHE) entrant dans le champ d'application du Référentiel général de sécurité (RGS) au titre du décret n°2010-112 du 2 février 2010

qui s'inscrivent dans le cadre de l'application des documents référencés au §2.1.2.2 ;

- Les certifications des prestataires de services de confiance (PSCO) entrant dans le champ d'application du règlement (UE) n°910/2014 (eIDAS)

qui s'inscrivent dans le cadre de l'application des documents référencés au §2.1.2.3 ;

- Les certifications des prestataires de services d'informatique en nuage selon le référentiel SecNumCloud

qui s'inscrivent dans le cadre de l'application des documents référencés au §2.1.2.4.

4. MODALITES D'APPLICATION

Ce document est applicable à compter du 01/01/2019.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Du fait de la refonte du document et par souci de lisibilité, les modifications n'y sont pas repérées.

Les principaux changements concernent :

- L'ajout du schéma de certification des prestataires de services en nuage selon le référentiel SecNumCloud.
- La séparation et l'apport de précisions sur les textes applicables pour les PASSI et pour les PSCE et PSHE entrant dans le champ d'application du décret n°2010-112 du 2 février 2010 (§2.1.2.1, §6.1 à 6.3)
- L'apport de précisions sur les exigences applicables pour les certifications des prestataires de services de confiance (PSCO) entrant dans le champ d'application du règlement (UE) n°910/2014 (eIDAS) aux §2.1.2.3 et 6.4
- La modification des modalités de réalisation des observations d'activités dans le cadre de la certification selon le RGS, le Règlement eIDAS ou les normes ETSI au §7.4.

6. EXIGENCES A SATISFAIRE PAR L'ORGANISME DE CERTIFICATION

Il appartient à tout organisme candidat ou accrédité de se tenir à jour des documents de référence cités au §2 et de prendre en compte la réglementation applicable en vigueur.

Seules les exigences spécifiques à chaque domaine ont été précisées, étant entendu que les exigences générales de la norme d'accréditation et les procédures en vigueur s'appliquent sans restriction.

6.1. Pour les PASSI entrant dans le champ d'application du décret n°2010-112 du 2 février 2010

Parmi les documents référencés au §2.1.2.1, les suivants s'appliquent en France :

- Décret n°2010-112 du 2 février 2010,
- [PASSI],
- [TRAME_PASSI],
- [QUAL_SERV_PROCESS],
- [QUAL_SERV_PORTEES],
- [QUAL_SERV_CE].

6.2. Pour les PASSI entrant dans le champ d'application du décret n°2015-350 du 27 mars 2015

Parmi les documents référencés au § 2.1.2.1, les suivants s'appliquent en France :

- Décret n°2015-350 du 27 mars 2015,
- [PASSI],
- [PASSI_LPM],
- [TRAME_PASSI],
- [QUAL_SERV_PROCESS],
- [QUAL_SERV_PORTEES],
- [QUAL_SERV_CE].

6.3. Pour les prestataires de service (PSCE ou PSHE) entrant dans le champ d'application du décret n°2010-112

Parmi les documents référencés au §2.1.2.1, les suivants s'appliquent en France :

- Décret n°2010-112 du 2 février 2010,
- [RGS],
- [QUAL_SERV_PROCESS],
- [QUAL_SERV_CE].

6.4. Pour les prestataires de service de confiance entrant dans le champ d'application du règlement (UE) n°910/2014 (eIDAS)

L'accréditation est délivrée par rapport à la norme NF EN ISO/CEI 17065, au document ETSI EN 319 403, exigences applicables à l'organisation, aux ressources et au processus de certification des OC, qui spécifie la norme NF EN ISO/CEI 17065, et aux exigences spécifiques de l'organe de contrôle de chaque État Membre pour chaque service identifié par l'organisme dans la demande d'accréditation.

Les exigences applicables aux prestataires de services sont définies par l'OC demandeur de l'accréditation pour chaque service dans son programme de certification.

Les exigences applicables aux prestataires sont à minima celles définies :

- Pour la certification électronique (signature) dans les documents ETSI EN 319 401, ETSI EN 319 411 parties 1 et 2 ;
- Pour l'horodatage électronique dans les documents ETSI EN 319 401 et ETSI EN 319 421,

Et tout autre norme ETSI identifiée par l'OC dans la demande d'accréditation.

Parmi les documents référencés au § 2.1.2.3, les documents complémentaires suivants s'appliquent en France :

- Pour chaque service : documents publiés par l'ANSSI, reprenant l'ensemble des exigences du règlement (UE) n°910/2014 eIDAS, et indiquant pour chacune d'entre elles les modalités pratiques permettant d'y apporter présomption de conformité
  - Prestataires de services de confiance qualifiés – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;
  - Services d'horodatage électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;
  - Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;
  - Services de validation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;

  - Services de conservation qualifiés des signatures et des cachets électroniques qualifiés – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;
  - Services d'envoi recommandé électronique qualifiés – critères d'évaluation de la conformité au règlement eIDAS – *version en vigueur* ;
  - Services d'horodatage électronique qualifiés – modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS – *version en vigueur* ;
  - Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS – *version en vigueur.*

- Document de l'ANSSI [CRITERES_OEC] : Organismes d'évaluation de la conformité des prestataires de service de confiance – Critères de reconnaissance au titre du règlement eIDAS.

6.5. Pour les prestataires de services d'informatique en nuage (SecNumCloud)

Parmi les documents référencés au §2.1.2.4, les suivants s'appliquent :

- Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences, version en vigueur,
- [QUAL_SERV_PROCESS],
- [QUAL_SERV_PORTEES],
- [QUAL_SERV_CE]

7. PROCESSUS D'ACCREDITATION

7.1. Généralité

Pour chaque évaluation, l'équipe d'évaluation comprend un ou plusieurs évaluateur(s) technique(s) compétent(s) en fonction de la portée d'accréditation demandée.

7.2. Portée d'accréditation

La portée d'accréditation est établie suivant le document CERT CPS INF 02.

Dans le cadre des demandes d'accréditation pour le règlement eIDAS, l'Organisme de Certification devra se rapprocher de l'organe de contrôle de chaque État Membre dans lequel il souhaite certifier des PSCO afin d'obtenir la liste des exigences applicables pour chaque service demandé, si celles-ci ont été définies. Il appartient ensuite aux OC de lister les normes et exigences applicables pour chaque service demandé.

7.3. Modalités d'évaluation

Toute demande d'accréditation en application des textes référencés au §2.1 sera traitée selon la procédure prévue dans le document CERT REF 05,

- comme une demande d'accréditation initiale si l'OC n'est pas accrédité selon l'ISO/CEI 17065, ou
- comme une demande d'extension majeure de la portée d'accréditation à un nouveau domaine (objet du présent document) si l'OC est accrédité selon l'ISO/CEI 17065.

Pour toute autre demande de la part d'OC déjà accrédités pour l'un des domaines, les extensions sont traitées selon le tableau ci-après.

- Pour un même service de confiance (RGS, eIDAS, ETSI) : extension mineure
- Pour changer de service de confiance (indépendamment du cadre RGS, eIDAS, ETSI): extension intermédiaire
- Pour passer de services de confiance à PASSI et inversement : extension majeure

Accréditation déjà octroyée / Accréditation demandée	PASSI décret n°2010-112	PASSI décret n°2015-350	PSCE décret n°2010-112	PSHE décret n°2010-112	PSCE Règlement (UE) n°910/2014	PSHE Règlement (UE) n°910/2014	eIDAS autre service de confiance	SecNum Cloud
PASSI décret n°2010-112		Mineure	Majeure	Majeure	Majeure	Majeure	Majeure	Majeure
PASSI décret n°2015-350	Mineure		Majeure	Majeure	Majeure	Majeure	Majeure	Majeure
PSCE décret n°2010-112	Majeure	Majeure		Intermédiaire	Mineure	Intermédiaire	Intermédiaire	Majeure
PSHE décret n°2010-112	Majeure	Majeure	Intermédiaire		Intermédiaire	Mineure	Intermédiaire	Majeure
PSCE Règlement (UE) n°910/2014	Majeure	Majeure	Mineure	Intermédiaire		Intermédiaire	Intermédiaire	Majeure
PSHE Règlement (UE) n°910/2014	Majeure	Majeure	Intermédiaire	Mineure	Intermédiaire		Intermédiaire	Majeure
eIDAS autre service de confiance	Majeure	Majeure	Intermédiaire	Intermédiaire	Intermédiaire	Intermédiaire	Intermédiaire	Majeure
SecNumCloud	Majeure	Majeure	Majeure	Majeure	Majeure	Majeure	Majeure	

Les extensions majeures et mineures sont décrites dans le règlement d'accréditation CERT REF 05.

La demande d'extension intermédiaire est traitée comme une demande d'extension mineure, à la différence que la décision d'extension doit être confirmée sur la base d'une observation d'activité de certification pour l'activité en question, à réaliser dans les 12 mois suivant la décision d'extension. Le rapport de l'observation correspondante est traité séparément du rapport « siège » par la Commission d'Accréditation qui propose un avis au Directeur Général du COFRAC sur cette extension.

7.4. Observation d'activité

Pour toute demande d'accréditation initiale ou d'extension majeure/intermédiaire ou de renouvellement, il doit être effectué une observation d'activité par domaine :

- Une pour les PASSI,
- Une dans le cadre du RGS (PSCE ou PSHE),
- Une dans le cadre du Règlement eIDAS (quel que soit le service).

Lors de chaque évaluation de surveillance, il doit être réalisé *a minima*:

- Une observation pour les certifications de PASSI à chaque surveillance,
- Une observation pour les certifications sous RGS ou eIDAS/ETSI.

Dans la mesure du possible il est observé des services certifiés différents au cours du cycle d'accréditation afin de garantir la représentativité de l'échantillon observé.

Pour chaque observation, l'OC communique à l'évaluateur en charge de l'observation le plan de l'audit observé, les rapports d'audit précédents (le cas échéant), la preuve de la compétence de l'équipe d'audit et la justification du calcul du temps d'audit.

Par activité de certification, on entend notamment un audit, un test ou une réunion d'un comité. Compte-tenu des durées standards des audits initiaux et de renouvellement de qualification, il est admis que les observations ne portent pas sur la totalité de l'audit sous réserve de l'acceptation de la structure permanente sur présentation du programme d'audit. A défaut, la totalité de l'audit sera observée.

Observation d'audit selon SecNumCloud

Il doit être réalisé une observation d'activités de certification selon le référentiel SecNumCloud à chaque évaluation (initiale, extension, surveillance ou renouvellement)

Chaque observation portera sur une partie de l'audit afin que l'audit de l'ensemble des exigences du référentiel SecNumCloud puisse être observé sur un cycle d'accréditation.

7.5. Attestation d'accréditation

L'attestation d'accréditation délivrée est établie selon le document CERT CPS INF 02.
Pour chaque domaine de certification, il est précisé le ou les service(s) pour le(s)quel(s) l'accréditation a été octroyée en cohérence avec la portée demandée.

7.6. Confidentialité – Echanges d'information

En application de l'article 11 du décret n°2010-112 du 2 février 2010 et de l'article 17 du décret n°2 015-350 du 27 mars 2015, le COFRAC doit informer sans délai l'ANSSI de toute décision d'octroi, d'extension, de réduction, de refus, de retrait ou de suspension d'accréditation d'un OC pour des PSCE et des PSHE entrant dans le champ d'application du décret n°2010-112 (RGS) ou pour des PASSI entrant dans le champ d'application du décret n°201 0-112 (RGS) ou du décret n°2015-350.

Le COFRAC informe sans délai la Commission Européenne et l'organe de contrôle compétent de toute décision d'octroi, d'extension, de réduction, de refus, de retrait ou de suspension d'accréditation d'un OC pour la certification des PSCO selon le Règlement eIDAS. Le COFRAC envoie une copie de l'attestation pour inscription de l'OC sur la liste de la Commission Européenne. (List of conformity assessment bodies (CABs) accredited against the requirements of the eIDAS Regulation https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation).

Le COFRAC informe sans délai l'ANSSI de toute décision d'octroi, d'extension, de réduction, de refus, de retrait ou de suspension d'accréditation d'un OC pour la certification des prestataires de services d'informatique en nuage (SecNumCloud).

7.7. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme certificateur

Les dispositions suivantes s'appliquent en complément de la procédure GEN PROC 03.

7.7.1 Dispositions à prendre en cas de suspension d'accréditation

Les actions à mettre en œuvre par l'organisme de certification concernant les certificats en vigueur émis sous accréditation sont établies par l'autorité compétente (par exemple l'ANSSI pour prestataires

qualifiés au titre des décrets n°2010-112 et n°2015 -350 ou du Règlement eIDAS) en fonction de la raison de la suspension qui est indiquée dans le courrier de notification de suspension.

7.7.2 Dispositions à prendre en cas de retrait de l'accréditation ou de cessation d'activité d'un organisme certificateur.

7.7.2.1 Retrait d'accréditation d'un organisme certificateur

L'organisme n'est plus autorisé à délivrer de certificats ni à maintenir les certificats existants. Il doit informer les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue.

Ce dernier doit alors demander à l'organisme de certification ayant délivré le certificat en cours de validité de lui adresser le dossier du client (rapports d'audits précédents, non conformités en suspens, plaintes reçues et suites données). Il peut également demander au client tous compléments d'informations nécessaires conformément au processus de certification sollicité.
Au cas où le certificateur « repreneur » serait dans l'impossibilité de se procurer le dossier du client auprès de l'organisme précédent, la demande de l'entreprise serait traitée comme une certification initiale en appliquant les procédures correspondantes.

Dans tous les cas, il revient à l'organisme certificateur « repreneur » d'évaluer les éléments fournis et d'établir si le cycle de certification peut être repris à la même étape de certification que celle dans laquelle il était auparavant opéré.

7.7.2.2 Cessation d'activité d'un organisme certificateur

L'organisme de certification doit informer les clients concernés dans les meilleurs délais pour qu'ils puissent s'adresser à un autre organisme de certification accrédité à cet effet, afin de transférer le cas échéant la certification détenue, dans les conditions énoncées au § 7.7.2.1.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant les activités de certification objet du présent document comme un domaine d'accréditation.