



Exigences spécifiques pour l'accréditation des organismes procédant à la certification de services de confiance numérique

CERT CPS REF 55 - Révision 00

LA VERSION ELECTRONIQUE FAIT FOI





SOMMAIRE

1. OBJET	3
2. REFERENCES ET DEFINITIONS.....	3
2.1. Références.....	3
2.2. Abréviations et définitions.....	4
3. DOMAINE D'APPLICATION.....	4
4. MODALITES D'APPLICATION.....	5
5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE.....	5
6. EXIGENCES ET REGLES A SATISFAIRE PAR L'OC.....	5
7. PROCESSUS D'ACCREDITATION	8
7.1. Généralités.....	9
7.2. Portée d'accréditation demandée.....	9
7.3. Modalités d'évaluation.....	9
7.4. Attestation d'accréditation.....	12
7.5. Confidentialité – Echange d'informations.....	12
7.6. Dispositions à prendre en cas de suspension, de retrait d'accréditation ou de cessation d'activité de l'organisme certificateur	12
8. MODALITES FINANCIERES.....	13
ANNEXE 1 : Exigences à satisfaire pour l'évaluation et la certification des prestations liées à la sécurité des systèmes d'information selon le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS » [EIDASv1].....	
	14



1. OBJET

Ce document définit les exigences à satisfaire et le processus d'accréditation pour l'évaluation et la certification de services de confiance numérique selon :

- Le Règlement (UE) n°910/2014 du 23/07/2014 (modalités précédemment définies dans le CERT CPS REF 33 et à présent en annexe du présent document)
- Le Règlement (UE) n°910/2014 du 23/07/2014 modifié par le Règlement (UE) 2024/1183 du 11/04/2024.
- Le Référentiel Général de Sécurité, version 2.0 du 13 juin 2014
- Le schéma de certification de « Certification composite de services pour les besoins des services de confiance numériques » de l'ANSSI tel que défini dans [SCHEMA-SERV].

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/IEC 17065 :2012 : « Évaluation de la conformité — Exigences pour les organismes certifiant les produits, les procédés et les services »

2.1.2. Autres textes de référence

Textes réglementaires

- 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. Ce règlement est appelé [EIDASv1] dans l'Annexe du document.
- 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, modifié par le Règlement (UE) 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n°910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique. Ce règlement est appelé [EIDASv2] dans l'ensemble de ce document.
- Référentiel général de sécurité, version 2.0 du 13 juin 2014, 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° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Ce référentiel est appelé [RGSv2] dans l'ensemble de ce document.

Textes de l'ANSSI

- [SCHEMA-SERV] Schémas de certification et de qualification de services, ANSSI, version en vigueur, disponible sur le site Internet de l'ANSSI <https://cyber.gouv.fr/>.



Lignes directrices de GLOBAL ACI

- [IAF MD2] renommé [Global ACI-TECH3-002] Document d'exigences pour le transfert d'une certification sous accréditation de systèmes de management disponible sur www.global-aci.org.

Note de transition

- [COFRAC-TRANSITION-EIDAS] Note de transition vers eIDAS V2 : Règlement (UE) 2024/1183 modifiant le Règlement (UE) 910/2014 disponible sur www.cofrac.fr.

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
GLOBAL ACI	Global Accreditation Cooperation Incorporated
OC	Organisme de Certification
RGS	Référentiel Général de Sécurité
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 la certification selon les domaines techniques suivants :

- Certification de services de confiance en conformité avec le référentiel [RGSv2] :
 - Service de certificats électroniques (PSCE) ;
 - Service d'horodatage électronique (PSHE) ;
- Certification de services de confiance en conformité avec le Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 [EIDASv2] pour les services de confiance **qualifiés** listés ci-après :
 - Service de délivrance de certificats **qualifiés** de signature électronique ;
 - Service de délivrance de certificats **qualifiés** de cachet électronique ;
 - Service de délivrance de certificats **qualifiés** d'authentification de site internet ;
 - Service de création d'horodatages électroniques **qualifiés** ;
 - Service d'envoi recommandé électronique ;
 - Service de validation de signatures électroniques **qualifiées** ;
 - Service de validation de cachets électroniques **qualifiés** ;
 - Service de conservation de signatures électroniques **qualifiées** ;
 - Service de conservation des cachets électroniques **qualifiés** ;
 - Service de gestion de dispositifs de création de signature électronique **qualifiés** à distance ;
 - Service de gestion de dispositifs de création de cachet électronique **qualifiés** à distance ;
 - Service de délivrance d'attestations électroniques d'attributs **qualifiés** ;
 - Service d'archivage électronique ;
 - Service d'enregistrement de données électroniques dans un registre électronique **qualifié** ;
- Certification de portefeuilles européens d'identité numérique pour les besoins de [EIDASv2] ;
- Certification de services de vérification d'identité pour les besoins des services de confiance au titre du règlement [EIDASv2] ;
- Certification composite de services pour les besoins de services de confiance numériques tel que défini dans [SCHEMA-SERV].



4. MODALITES D'APPLICATION

Ce document est applicable à compter du 15/10/2026.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Il s'agit de l'édition initiale du document.

6. EXIGENCES ET REGLES A SATISFAIRE PAR L'OC

Il appartient à tout organisme candidat ou accrédité d'appliquer les versions à jour des documents de référence cités au §2 et de prendre en compte la réglementation applicable en vigueur.

En particulier, le document [SCHEMA-SERV] définit les exigences applicables aux organismes de certification.

Dans la suite du document, seules les exigences spécifiques ont été indiquées, étant entendu que les exigences générales citées au §2 s'appliquent.

Ces tableaux sont une aide à la compréhension de l'interaction des différentes exigences applicables aux OC mais ne constituent pas une liste exhaustive et restent à valeur indicative.

6.1. Certification de services de confiance en conformité avec le référentiel [RGSv2]

Chapitre de la norme NF EN ISO/IEC 17065 :2012	Autres documents applicables et commentaires éventuels
7.7 Documents de certification	[SCHEMA-SERV]
7.8 Annuaire des produits certifiés	[SCHEMA-SERV]



6.2. Pour la certification de services de confiance en conformité avec le Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 [EIDASv2], pour tous les services de confiance qualifiés listés au §3

Chapitre de la norme NF EN ISO/IEC 17065 :2012	Règlement d'exécution (UE) 2025/2162 (en lien avec l'article 20 §4 du Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 (eIDAS V2))	Norme ETSI EN 319 403-1 version 2.3.1	Autres documents applicables et commentaires éventuels
3.9 Programme de certification			[SCHEMA-SERV]
4.2 Gestion de l'impartialité		4.2.1 Activities not conflicting with impartiality	
4.6 Informations accessibles au public	Article 5 §1 Article 6 §10		
6.1 Personnel de l'organisme de certification 6.2 Ressources pour l'évaluation	Article 6 §5.f	6.1.2 Management of competence for personnel involved in the audit process 6.2.1 Internal resources	
6.2.2 Ressources externes (externalisation)	Article 5 §2		
7.1 Généralités		7.1 General requirements	
7.3 Revue de la demande		7.3 Application Review	
7.4 Evaluation	Article 6 Article 7 Annexe III Article 5 §3	7.4 Audit	[SCHEMA-SERV]
7.4.5 Transfert de certification			[SCHEMA-SERV] ; [Global ACI-TECH3-002]
7.5 Revue		7.5 Review	
7.6 Décision de certification	Article 5 §3 Article 6 §7	7.6 Certification decision	
7.7 Documents de certification		7.7 Certification documentation	[SCHEMA-SERV]
7.8 Annuaire des produits certifiés	Article 5 §1	7.8 Directory of certified products	
7.9 Surveillance	Article 6 §5.d Article 6 §11	7.9 Surveillance	[SCHEMA-SERV]
7.10 Changements ayant des conséquences sur la certification	Article 6 §5.e Article 6 §6	7.10 Changes affecting certification	



6.3. Pour la certification de services de vérification d'identité pour les besoins des services de confiance au titre du règlement [EIDASv2] et pour la certification composite de services pour les besoins de services de confiance numériques

Chapitre de la norme NF EN ISO/IEC 17065 :2012	Norme ETSI EN 319 403-1 version 2.3.1	Autres documents applicables et commentaires éventuels
3.9 Programme de certification		[SCHEMA-SERV]
4.2 Gestion de l'impartialité	4.2.1 Activities not conflicting with impartiality	
4.6 Informations accessibles au public		
6.1 Personnel de l'organisme de certification 6.2 Ressources pour l'évaluation	6.1.2 Management of competence for personnel involved in the audit process 6.2.1 Internal resources	
7.1 Généralités	7.1 General requirements	
7.3 Revue de la demande	7.3 Application Review	
7.4 Evaluation	7.4 Audit	
7.4.5 Transfert de certification		[SCHEMA-SERV] ; [Global ACI-TECH3-002]
7.5 Revue	7.5 Review	
7.6 Décision de certification	7.6 Certification decision	
7.7 Documents de certification	7.7 Certification documentation	[SCHEMA-SERV]
7.8 Annuaire des produits certifiés	7.8 Directory of certified products	[SCHEMA-SERV]
7.9 Surveillance	7.9 Surveillance	[SCHEMA-SERV]
7.10 Changements ayant des conséquences sur la certification	7.10 Changes affecting certification	



6.4. Pour la certification de portefeuilles européens d'identité numérique pour les besoins de [EIDASv2]

Chapitre de la norme NF EN ISO/IEC 17065 :2012	Règlement d'exécution 2024/2981 du 28 novembre 2024 (en lien avec l'article 5 quater, paragraphe 6 du Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 (eIDAS V2))	Autres documents applicables et commentaires éventuels
3.9 Programme de certification		[SCHEMA-SERV]
4.1.3 Utilisation de marque de conformité		[SCHEMA-SERV]
4.5 Confidentialité	Article 11 Article 14 Article 20 Annexe VIII	
6.2.2 Ressources externes	Article 10	
6.1 et 6.2.1 Personnel de l'OC - Ressources internes	Article 9 §2	
7.4 Evaluation	Article 3 §6 Article 3 §7 Article 13 Article 17 Annexe II Annexe III Annexe IV Annexe VI Annexe VIII Annexe IX	
7.4.5 Transfert		[SCHEMA-SERV] ; [Global ACI-TECH3- 002]
7.4.9 Résultats de l'évaluation	Revue de la conformité à l'Article 8	
7.7 Document de certification	Article 14 Annexe VII Annexe VIII	[SCHEMA-SERV]
7.9 Surveillance	Article 9 §3 Article 16 Article 18	[SCHEMA-SERV]
7.10 Changement ayant des conséquences sur la certification	Article 5	
7.11 Résiliation, réduction, suspension ou retrait de certification	Article 12	
7.12 Enregistrements	Article 19	
7.13 Plaintes et appels	Article 15	
Exigences du système de management	Article 4 §4 Article 4 §5	

7. PROCESSUS D'ACCREDITATION

Le processus d'accréditation décrit dans les règlements d'accréditation CERT REF 05, GEN REF 06 et CERT REF 60 s'applique, avec les précisions et spécificités décrites dans les paragraphes suivants.



7.1. Généralités

Les domaines d'accréditation définis au §3 sont considérés comme cinq domaines techniques d'accréditation distincts.

7.2. Portée d'accréditation demandée

La portée d'accréditation est établie selon le document de nomenclature CERT CPS INF 02.

Pour le domaine de la « Certification composite de services pour les besoins de services de confiance numériques », la portée d'accréditation délivrée par le Cofrac est considérée comme étant en portée flexible de type 2 et doit être gérée par l'OC conformément au document CERT REF 08.

La portée d'accréditation n'est donc pas détaillée pour ce domaine technique. Il revient à l'OC de tenir à jour sa portée détaillée, en cohérence avec les libellés des certificats émis ; elle doit identifier la/les norme(s) ETSI (référence et version selon la liste définie dans le document [SCHEMA-SERV]) pour lesquelles l'organisme de certification est capable d'émettre des décisions de certification.

Les autres domaines techniques sont considérés comme étant en portée flexible de type 1.

7.3. Modalités d'évaluation

7.3.1 Modalités de démarrage

En accord avec le document [SCHEMA-SERV], les organismes de certification ayant obtenu la recevabilité opérationnelle de leur demande d'accréditation pour la certification selon l'un des domaines techniques listés au §3 sont autorisés à démarrer le processus de certification et à prendre des décisions de certification mais ne pourront émettre de certificats sous accréditation qu'une fois l'accréditation obtenue.

Après recevabilité favorable de la demande d'accréditation par l'instance nationale d'accréditation, les organismes certificateurs en cours de demande d'accréditation sont autorisés à délivrer des certificats pendant douze (12) mois.

Les certificats émis pendant cette période pourront être réémis sous accréditations s'ils ont été initialement délivrés dans les mêmes conditions que celles ayant permis de prononcer l'accréditation.

7.3.2 Modalités de candidature

Toute demande d'accréditation pour la délivrance de certification de services de confiance tels que spécifiés au §3 sera traitée, conformément au CERT REF 05, GEN REF 06 et CERT REF 60 comme :

- une demande d'accréditation initiale si l'OC n'est pas accrédité selon la NF EN ISO/IEC 17065 ;
- comme une extension à un nouveau domaine technique si l'OC est déjà accrédité selon la NF EN ISO/IEC 17065 pour des activités autres que celles objets du présent document. Dans ce cas, l'évaluation doit inclure à minima un examen de traçabilité dossiers et une observation d'activité ;
- une demande d'extension de la portée d'accréditation au sein d'un domaine technique déjà accrédité, si l'OC est déjà accrédité selon la NF EN ISO/IEC 17065 selon un des domaines techniques listés au §3. L'extension sera traitée à minima selon les modalités du Tableau 1.

Les documents de candidature à adresser au Cofrac sont ceux prévus dans le formulaire de demande CERT FORM 29 pour une recevabilité obligatoire pour exercer les activités.



Pour toute demande d'accréditation concernant le domaine technique de la « Certification de services de confiance en conformité avec le Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 [EIDASv2] », l'organisme doit communiquer, en complément des éléments prévus dans le formulaire de candidature CERT FORM 29 :

- la procédure de qualification des auditeurs garantissant la prise en compte des exigences du point 5.f de l'article 6 du Règlement d'exécution (UE) 2025/2162 de la Commission du 27 octobre 2025 ;
- les preuves de la compétence de deux auditeurs.

Pour le domaine technique de la certification de portefeuilles européens d'identité numériques pour les besoins du règlement [EIDASv2], seule l'ANSSI peut effectuer une demande d'accréditation sur le schéma sous accréditation comme précisé dans [SCHEMA-SERV].

Tableau 1 – modalités d'extension à un nouveau domaine technique listé au §3

Accréditation déjà octroyée / Accréditation demandée	Certification de services de confiance en conformité avec le référentiel [RGSv2] PSHE/PSCE	Certification de services de confiance en conformité avec [EIDASv2]	Certification de services de vérification d'identité pour les besoins des services de confiance au titre du règlement [EIDASv2]	Certification composite de services pour les besoins de services de confiance numériques.	Certification de portefeuilles européens d'identité numérique pour les besoins du règlement [EIDASv2]
Certification de services de confiance en conformité avec le référentiel [RGSv2] PSHE/PSCE	Pour les extensions à un nouveau service : voir le tableau 2	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.		Evaluation documentaire.
Certification de services de confiance en conformité avec [EIDASv2]	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.	Pour les extensions à de nouveaux services : voir le tableau 3	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	Une observation sera ajoutée à l'évaluation périodique suivante.
Certification de services de vérification d'identité pour les besoins des services de confiance au titre du règlement [EIDASv2]	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.		Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.
Certification composite de services pour les besoins de services de confiance numériques	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.				
Certification de portefeuilles européens d'identité numérique pour les besoins du règlement [EIDASv2]	Sans objet : seuls les organismes d'évaluation de la conformité désignés par les Etats Membres peuvent demander une accréditation pour la certification des portefeuilles européens d'identité numérique. Le cas échéant, la demande est considérée comme une demande d'accréditation initiale.				



Tableau 2 – Modalités d'extension d'accréditation dans le domaine des certifications de services de confiance en conformité avec le référentiel [RGSv2] :

- Service de certificats électroniques (PSCE) ;
- Service d'horodatage électronique (PSHE).

Accréditation déjà octroyée / Accréditation demandée	Certification de PSCE au titre du [RGSv2]	Certification de PSHE au titre du [RGSv2]
Certification de PSCE au titre du [RGSv2]		Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante
Certification de PSHE au titre du [RGSv2]	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante	

Tableau 3 Modalités d'extension d'accréditation dans le domaine des certifications de service de confiance en conformité avec le Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 [EIDASv2] pour les services de confiance qualifiés listés au §3

Accréditation déjà octroyée / Accréditation demandée	Certification de services de confiance en conformité avec [EIDASv2] Tous les services hormis services d'archivage électronique et services d'enregistrement de données électroniques dans un registre électronique qualifié	Certification de services d'archivage électronique	Certification de services d'enregistrement de données électroniques dans un registre électronique qualifié
Certification de service de confiance en conformité avec [EIDASv2] Tous les services hormis services d'archivage électronique et services d'enregistrement de données électroniques dans un registre électronique qualifié	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante.	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.
Certification de services d'archivage électronique	Evaluation documentaire. Une observation sera ajoutée à l'évaluation périodique suivante		
Certification de services d'enregistrement de données électroniques dans un registre électronique qualifié		Evaluation au siège (examens de traçabilité de dossiers) et une observation d'activité.	

7.3.3 Evaluations périodiques

Chaque domaine technique de la portée d'accréditation est évalué à chaque évaluation périodique. Pour les domaines techniques impliquant un ou plusieurs services, les évaluations (au siège et les observations d'activités) couvrent tous les services de la portée d'accréditation sur un cycle d'accréditation.

7.3.4 Observations d'activités de certification

Pour le domaine technique de la Certification de services de confiance en conformité avec le Règlement (UE) n°910/2014 modifié par le Règlement (UE) 2024/1183 [EIDASv2] pour les services de confiance



qualifiés, il doit être réalisé a minima une observation d'activité à chaque évaluation du cycle (initiale, surveillance ou renouvellement).

Pour les domaines techniques de :

- La Certification de services de confiance en conformité avec le référentiel [RGSv2] ;
- La Certification de services de vérification d'identité pour les besoins des services de confiance au titre du règlement [EIDASv2] ;
- La Certification composite de services pour les besoins de services de confiance numériques telle que définie dans [SCHEMA-SERV] ;

Il doit être réalisé a minima deux observations d'activité par domaine technique par cycle d'accréditation.

Pour le domaine technique de la Certification de portefeuilles européens d'identité numérique au titre de [EIDASv2], la 1^{ère} observation d'activité (évaluation initiale ou extension) doit être réalisée dans les 12 mois suivant la notification de la recevabilité opérationnelle de la demande.

Par la suite, il doit être réalisé a minima deux observations d'activité par cycle d'accréditation.

Dans la mesure du possible, chaque observation concerne un service différent, un client différent, un auditeur différent, et est sélectionnée de façon à couvrir un maximum de services de confiance de la portée d'accréditation.

Dans le cadre des extensions à de nouveaux domaines techniques ou à de nouveaux services, les observations à réaliser sont définies dans les tableaux 1, 2 et 3 au §7.3.2. Ces observations sont réalisées en complément de celles prévues lors de l'évaluation périodique du cycle d'accréditation. Elles peuvent être combinées si les audits couvrent tous les domaines techniques et/ou services devant faire l'objet d'une observation d'activité.

Les observations peuvent couvrir tout ou partie de l'activité de certification observée si la partie observée est représentative de l'audit.

7.4. Attestation d'accréditation

L'attestation d'accréditation délivrée est établie selon le document de nomenclature CERT CPS INF 02.

7.5. Confidentialité – Echange d'informations

Les modalités d'échange d'informations sont spécifiées dans [SCHEMA-SERV].

Le COFRAC informe sans délai l'organe de contrôle compétent (ANSSI) de toute décision d'octroi, d'extension, de réduction, de refus, de suspension ou de retrait d'accréditation d'un organisme de certification selon le Règlement [EIDAS_V2].

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

Les dispositions spécifiées dans [SCHEMA-SERV] pour chacune des situations s'appliquent en complément de la procédure GEN PROC 03.



Le Cofrac informe sans délai les autorités compétentes de toute mesure de suspension ou de retrait d'accréditation d'un organisme certificateur.

7.6.1 Dispositions à prendre en cas de suspension d'accréditation

Les actions à mettre en œuvre par l'organisme concernant les certificats en vigueur émis sous accréditation sont établies au cas par cas en fonction de la raison de la suspension et sont indiquées dans le courrier de notification de suspension.

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

7.6.2.1 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 l'identique.

7.6.2.2 Cessation d'activité d'un organisme certificateur

L'organisme certificateur 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 § 7.6.2.1.

8. MODALITES FINANCIERES

Les modalités énoncées dans les documents CERT REF 06 et CERT REF 07 s'appliquent, en considérant en considérant les domaines d'accréditation définis au §3 comme des domaines techniques d'accréditation distincts.



ANNEXE 1 : Exigences à satisfaire pour l'évaluation et la certification des prestations liées à la sécurité des systèmes d'information selon le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS » [EIDASv1]

1. Contexte

Les modalités décrites dans cette annexe reprennent celles définies précédemment dans le CERT CPS REF 33 pour l'évaluation et la certification des prestations liées à la sécurité des systèmes d'information selon le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS » [EIDASv1].

Ces modalités sont valides jusqu'à la fin de la période de transition vers [EIDASv2], à savoir le 17/05/2027, comme mentionné dans la note publiée par le Cofrac et disponible sur son site internet :

https://cofrac-corporateprod-resources-files.s3.amazonaws.com/Note_pour_la_transition_eIDAS_v2_FINAL.pdf

Comme précisé dans cette note, l'instruction des demandes d'accréditation initiale ou d'extension reçues à compter du 1er janvier 2026 et leur évaluation subséquente seront réalisées en prenant en compte les nouvelles exigences introduites par le Règlement (UE) 2024/1183 pour les services listés dans le document de nomenclature CERT CPS INF 02.

Par conséquent, seuls sont repris ici les textes de référence applicables pour les organismes accrédités selon le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS » [EIDASv1].

Les modalités d'évaluation applicables sont celles définies dans le CERT REF 05 / CERT REF 60 pour les organismes de certification qui resteraient accrédités uniquement pour la certification des prestations liées à la sécurité des systèmes d'information selon le Règlement (UE) n°910/2014 du 23/07/2014 « eIDAS » jusqu'à la fin de la période de transition.

2. Textes de référence 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-Stamped, (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 [EIDASv1], 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.



3. Exigences à 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 [de cette annexe] et de prendre en compte la réglementation applicable en vigueur.

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 toute 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.



4. Observation d'activité

Lors de chaque évaluation de surveillance, il doit être réalisé a minima une observation pour les certifications selon [EIDASv1]. 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.

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.

LA VERSION ELECTRONIQUE FAIT FOI