Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de services de confiance qualifiés

Critères d'évaluation de la conformité au règlement eIDAS

Version 1.3 du 11 avril 2025

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
04/05/2016	1.0	Version pour application au 1er juillet 2016.	ANSSI
03/01/2017	1.1	Version pour application au 31 janvier 2017. *Modifications :* - *Précisions relatives au maintien du statut qualifié et à l'inscription dans la liste de confiance ;* - *Précisions relatives aux modalités de certification des équipements cryptographiques et à l'emploi de la cryptographie ;* - *Modifications mineures et clarifications.*	ANSSI
28/03/2017	1.2	Version pour application au 3 août 2017. *Modifications :* - *Prise en compte de la nouvelle version du guide d'hygiène informatique ;* - *Prise en compte de la nouvelle version du référentiel du SOG-IS relatif à l'emploi des mécanismes cryptographiques ;* - *Ajout de précisions sur la liste des changements importants nécessitant une notification à l'ANSSI.*	ANSSI
11/04/2025	1.3	Version pour application dès publication. *Modifications :* - *Modification de l'adresse URL du SOGIS ;* - *Modification de l'adresse URL de l'ANSSI .*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

supervision-eIDAS@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Objet

Dans le cadre du règlement [eIDAS], l'ANSSI, désignée comme organe de contrôle par la note des autorités françaises [NOTIFICATION], a la charge de contrôler le respect des exigences du règlement par les prestataires de service de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

La présente note décrit les exigences générales relatives à la qualification selon le règlement [eIDAS] de l'ensemble des prestataires de services de confiance, indépendamment de la nature des services de confiance qualifiés qu'ils fournissent.

Ces exigences générales sont complétées par les exigences spécifiques applicables à chaque type de service de confiance qualifié, faisant l'objet des documents distincts [eIDAS_DELIV_CERT], [eIDAS_HORO], [eIDAS_VAL_SIGN], [eIDAS_CONS_SIGN] et [eIDAS_ENVOI_RECO].

Note : Dans le cas où le service de confiance bénéficie des modalités de transition de la qualification selon le [RGS] vers la qualification selon le règlement [eIDAS], telles que précisées dans les notes [PSCE_RGS_eIDAS] et [PSHE_RGS_eIDAS], le présent document n'est pas applicable.

I.2. Cadre juridique

Les prestataires de services de confiance qualifiés, respectant les exigences spécifiées au chapitre II du présent document ainsi que les exigences spécifiques à chaque service de confiance qualifié qu'ils fournissent, bénéficient des effets juridiques prévus par le règlement [eIDAS] pour les services de confiance qualifiés.

Ces effets juridiques sont précisés dans les référentiels d'exigences spécifiques applicables à chacun des services de confiance qualifiés.

I.3. Mise à jour

L'opportunité de la mise à jour de ce document est évaluée par l'ANSSI et peut notamment être le fait d'une évolution du cadre réglementaire ou normatif lié au règlement [eIDAS] ou d'une évolution de l'état de l'art.

L'ANSSI précise la date d'effet de chaque mise à jour et les modalités de transition le cas échéant.

I.4. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
CCRA	*Common Criteria Recognition Agreement.*
CESTI	Centre d'Evaluation de la Sécurité des Technologies de l'Information.
OID	*Object IDentifier*.
PSCo	Prestataire de Services de Confiance.
SOG-IS	*Senior Officials Group – Information systems Security*.

II. Exigences relatives aux prestataires de services de confiance qualifiés

II.1. Modalités de qualification

II.1.1. Processus de qualification

L'ANSSI prend une décision de qualification d'un prestataire de services de confiance sur la base d'un rapport d'évaluation de la conformité élaboré par un organisme d'évaluation de la conformité répondant aux critères définis dans la note [CRITERES_OEC].

Ce rapport d'évaluation doit permettre de vérifier le respect de l'ensemble des exigences applicables au prestataire de service de confiance telles que spécifiées dans la présente note, ainsi que des exigences applicables au service de confiance faisant l'objet de la demande de qualification.

Le processus de qualification est décrit dans le document [QUALIF_SERV].

II.1.2. Durée de validité et maintien de la qualification

La qualification du prestataire de services de confiance est délivrée pour une durée maximale de deux ans, conformément à l'article 20 du règlement [eIDAS].

Pour permettre un maintien ininterrompu du statut qualifié d'un service de confiance, un rapport d'évaluation de la conformité établi par un organisme répondant aux critères de [CRITERES_OEC] doit être transmis à l'ANSSI trois mois au moins avant l'expiration de la qualification.

II.1.3. Considérations relatives à l'inscription dans la liste de confiance

L'identification d'un service de confiance qualifié dans la liste de confiance doit respecter les exigences définies dans la clause 5.5.3 du standard [TS_119_612].

En particulier, il est attendu que la valeur de l'attribut « *Organization* », figurant dans le certificat électronique identifiant le service de confiance qualifié, corresponde au nom du prestataire de services de confiance qualifié tel qu'indiqué dans le champ « *TSP Name* » de la liste de confiance.

Les référentiels d'exigences publiés par l'ANSSI précisent, pour chaque service de confiance qualifié selon le règlement, les moyens autorisés d'identification du service pour son inscription dans la liste de confiance.

Note : Le périmètre de l'évaluation de la conformité doit être cohérent avec le niveau de précision de l'identifiant retenu pour le service de confiance qualifié dans la liste de confiance qualifié.

L'inscription, dans la liste de confiance, d'un nouvel élément d'identification pour un service déjà qualifié (*par exemple, l'ajout d'un nouveau certificat électronique d'unité d'horodatage ou d'autorité de certification, ou d'un nouvel OID de politique de certification)* doit faire l'objet d'une demande à l'ANSSI suivant les modalités de contact définies dans [QUALIF_SERV]. Il est recommandé de prévoir un délai minimal de trois mois avant mise en service de ces nouveaux éléments, permettant l'instruction de la demande par l'ANSSI.

II.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences du règlement [eIDAS] applicables à l'ensemble des prestataires de services de confiance qualifiés, spécifiées dans les articles suivants :

- 5(1) Protection et traitement des données à caractère personnel ;
- 13(2) Limitation de responsabilités ;
- 15 Accessibilité ;
- 19(1) Gestion des risques ;
- 19(2) Notification des incidents ;
- 24(2).a Information de l'organe de contrôle relative aux modifications des services ;
    - b Expertise, fiabilité, expérience et qualification des personnels et sous-traitants ;
    - c Maintien de ressources financières suffisantes et/ou assurance responsabilité ;
    - d Information des conditions et limites d'utilisation des services ;
    - e Utilisation de produits et systèmes fiables, sécurité et fiabilité des processus ;
    - f Utilisation de systèmes fiables pour le stockage des données ;
    - g Mesures contre la falsification et le vol des données ;
    - j Traitement licite des données à caractère personnel.

Le respect de la norme [EN_ 319_401] et des compléments précisés dans le chapitre II.3 du présent document permet d'apporter une présomption de conformité à ces exigences.

Note : L'article 24(2).e fait également l'objet de précisions dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

La conformité aux articles 24(2).h et 24(2).i n'est pas abordée dans le présent document. Elle est traitée dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

II.3. Compléments à la norme [EN_ 319_401]

II.3.1. Compléments relatifs à la notification des changements apportés aux services fournis

En cas de modification importante dans la fourniture de ses services de confiance qualifiés, le PSCo doit informer l'ANSSI selon les modalités décrites dans le document [QUALIF_SERV].

Ces modifications importantes comprennent notamment, sans s'y limiter :

- les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
- les changements de sous-traitants ;
- les modifications des conditions d'hébergement ;
- les changements de matériels cryptographiques ;
- les modifications d'architecture technique ;
- les changements de procédures d'enregistrement et d'identification ;
- les changements dans la gouvernance du PSCo.

Les modifications entrainant des changements dans la liste de confiance publiée par l'ANSSI doivent être notifiées dans les meilleurs délais.

Le PSCo doit adresser à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés, impactant les constats présentés dans le rapport d'évaluation de la conformité, à une fréquence annuelle.

II.3.2. Compléments relatifs aux systèmes fiables pour le stockage des données

Le PSCo doit utiliser des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière à ce que :

- les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- seules des personnes autorisées puissent introduire et modifier les données conservées ;
- l'authenticité de ces données puisse être vérifiée.

II.3.3. Compléments au chapitre 5 de la norme [EN_ 319_401] : « *Risk Assessment* »

Le PSCo doit effectuer une analyse de risques sur le système d'information utilisé pour mettre en œuvre le service de confiance et procéder à son homologation conformément au guide [HOMOLOGATION]. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

Le PSCo doit évaluer l'opportunité de mettre à jour l'analyse de risques tous les ans.

Le PSCo doit mettre à jour l'analyse de risques à chaque modification ayant un impact important sur le service de confiance fourni, notamment en cas de modification des politiques ou pratiques relatives à la fourniture du service.

L'analyse de risque et la décision d'homologation doivent être jointes au rapport d'évaluation de la conformité transmis lors de la demande de qualification.

II.3.4. **Compléments au chapitre 7 de la norme [EN_ 319_401] : « *TSP Management and Operation* »**

§ 7.2.i : *« Human resources »*

Le PSCo doit mettre en œuvre tous les moyens légaux dont il peut disposer pour s'assurer de l'honnêteté de ses personnels. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ses personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire. L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

§ 7.4 : *« Access control »*

Le PSCo doit appliquer l'ensemble des règles définies dans le guide d'hygiène informatique [GH] publié par l'ANSSI, pour le niveau « standard ».

Il est recommandé d'appliquer les mesures de niveau « renforcé ».

§ 7.9 : *« Incident management »*

Le PSCo doit notifier à l'ANSSI dans un délai maximal de 24 heures après en avoir eu connaissance toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Cette notification est réalisée au moyen du formulaire mis en ligne sur le site de l'ANSSI, selon les modalités définies dans [QUALIF_SERV].

II.3.5. **Compléments relatifs à la certification des modules cryptographiques**

Les fonctions cryptographiques sensibles[1]doivent être mises en œuvre dans des modules cryptographiques répondant aux critères définis dans le tableau ci-dessous[2] :

Labellisation	Schéma	Référentiel	Commentaire / modalités
Certification Critères Communs[3]	ANSSI	Profils de protection reconnus par l'ANSSI, référencés sur le site www.cyber.gouv.fr	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	SOG-IS	Profils de protection HSM[4] recommandés sur le site https://sogis.eu	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	SOG-IS	Cible de sécurité vérifiée par l'ANSSI comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences du règlement.	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	CCRA	Cible de sécurité vérifiée par l'ANSSI comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences du règlement.	L'ANSSI demande à ce que les travaux correspondant aux augmentations non reconnues dans le cadre du CCRA soient réalisés dans un schéma du SOG-IS (avec fourniture du rapport technique d'évaluation au CESTI en charge de l'évaluation et au centre de certification).
Autre	Le demandeur doit fournir un argumentaire visant à démontrer à l'ANSSI que sa méthode d'évaluation, le laboratoire utilisé, le référentiel d'évaluation, etc. sont de même niveau qu'une certification Critères Communs réalisées dans le cadre du SOG-IS selon l'un des profils de protection reconnus par l'ANSSI. Le rapport d'évaluation doit être fourni à l'ANSSI pour analyse. L'ANSSI se réserve le droit de demander des analyses complémentaires aux frais du demandeur dans un laboratoire agréé et reconnu compétent pour ce type de produit au sein du SOG-IS.		

[1] Les référentiels d'exigences applicables à chaque type de service de confiance qualifié précisent les fonctions cryptographiques sensibles concernées selon le cas.

[2] Dans le cas particulier des fonctions de signature électronique qualifiée ou de cachet électronique qualifié, le dispositif de création de signature ou de cachet électronique qualifié utilisé doit être certifié conformément à l'article 30 du règlement [eIDAS].

[3] La certification selon les Critères Communs doit avoir une ancienneté inférieure à 10 ans.

[4] L'ANSSI vérifiera que le profil de protection est bien approprié pour le cas d'usage prévu du module cryptographique au sein de l'environnement du PSCo.

II.3.6. **Compléments relatifs aux algorithmes et mécanismes cryptographiques**

Les algorithmes et mécanismes cryptographiques mis en œuvre doivent être conformes aux spécifications du document [SOGIS-CRYPTO].

Pour les modules cryptographiques employés par le PSCo, certifiés conformément aux dispositions du chapitre II.3.5 du présent document, la vérification de la conformité à cette exigence nécessite, dans le cadre de leur certification :

- une analyse théorique des mécanismes cryptographiques mis en œuvre ; et
- une expertise de l'implémentation de ces mécanismes dans le module cryptographique.

II.3.7. **Langue des documents publiés par le PSCo**

Les documents publiés par le prestataire de services de confiance à destination du public (conditions générales d'utilisation et politiques relatives à la fourniture des services) doivent être rédigés en langue française.

En complément, il est recommandé qu'une version rédigée en langue anglaise de ces documents soit mise à disposition du public.

Annexes

I. Annexe 1 Références documentaires

Renvoi	Document
[CRITERES_OEC]	Organismes d'évaluation de la conformité – Critères de reconnaissance au titre du règlement eIDAS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[eIDAS]	Règlement n°910/2014 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 n°1999/93/CE. Disponible sur http://www.europa.eu
[eIDAS_DELIV_CERT]	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. Disponible sur https://cyber.gouv.fr/
[eIDAS_HORO]	Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[eIDAS_VAL_SIGN]	Services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[eIDAS_CONS_SIGN]	Services de conservation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[eIDAS_ENVOI_RECO]	Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[EN_319_401]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[GH]	Guide d'hygiène informatique. Disponible sur https://cyber.gouv.fr/
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, version en vigueur. Disponible sur https://cyber.gouv.fr/
[NOTIFICATION]	Note des autorités française du 17 février 2015 à la Commission, désignant l'ANSSI comme organe de contrôle au titre du règlement eIDAS.
[PSCE_RGS_EIDAS]	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. Disponible sur https://cyber.gouv.fr/

Renvoi	Document
[PSHE_RGS_EIDAS]	Services d'horodatage électronique qualifiés – Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur. Disponible sur https://cyber.gouv.fr/
[QUALIF_SERV]	Processus de qualification d'un service, version en vigueur. Disponible sur https://cyber.gouv.fr/
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version en vigueur. Disponible sur https://sogis.eu/
[TS_119_612]	ETSI TS 119 612 v2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI); Trusted Lists.

II. Annexe 2 Couverture des exigences du règlement [eIDAS]

Article	Exigence du règlement eIDAS	Clauses applicables des normes européennes	Chapitres applicables du présent document
5(1)	Protection et traitement des données à caractère personnel	[EN_319_401] Clause 7.13	*Pas de complément à la norme*
13(2)	Limitation de responsabilités	[EN_319_401] Clause 6.2	*Pas de complément à la norme*
15	Accessibilité	[EN_319_401] Clause 7.13	Chapitre II.3.7
19(1)	Gestion des risques	[EN_319_401] Clauses 5, 6.3, et 7.1 à 7.8	Chapitres II.3.3 et II.3.4
19(2)	Notification des incidents	[EN_319_401] Clause 7.9	Chapitre II.3.4
24(2).a	Information de l'organe de contrôle relative aux modifications des services	[EN_319_401] Clause 7.12	Chapitre II.3.1
24(2).b	Expertise, fiabilité, expérience et qualification des personnels et sous-traitants	[EN_319_401] Clause 7. 2	Chapitre II.3.4
24(2).c	Maintien de ressources financières suffisantes et/ou assurance responsabilité	[EN_319_401] Clause 7. 1.1	*Pas de complément à la norme*
24(2).d	Information des conditions et limites d'utilisation des services	[EN_319_401] Clause 6.2	*Pas de complément à la norme*
24(2).e	Utilisation de systèmes et produits fiables	[EN_319_401] Clause 7.7	Chapitres II.3.5 et II.3.6
24(2).f	Utilisation de systèmes fiables pour le stockage des données	*Non couvert*	Chapitres II.3.2 et II.3.4
24(2).g	Mesures contre la falsification et le vol des données	[EN_319_401] Clauses 7.6 et 7.7	*Pas de complément à la norme*
24(2).j	Traitement licite des données à caractère personnel	[EN_319_401] Clause 7.13	*Pas de complément à la norme*