Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Services d'envoi recommandé électronique qualifiés

Critères d'évaluation de la conformité au règlement eIDAS

Version 1.0 du 3 janvier 2017

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
23/06/2016	0.3	*Version de travail pour commentaires.*	ANSSI
03/01/2017	1.0	Version pour application au 31 janvier 2017. *Modifications :* - *Précisions relatives à l'inscription dans la liste de confiance ;* - *Modifications et précisions relatives à l'identification de l'expéditeur et du destinataire ;* - *Modifications mineures et clarifications.*	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 la conformité des services de confiance qualifiés qu'ils fournissent.

La présente note décrit les critères d'évaluation de la conformité aux exigences du règlement [eIDAS] des services d'envoi recommandé électronique qualifiés. Ces exigences s'appliquent de manière cumulative avec celles décrites dans la note [PSCO_QUALIF], applicables à l'ensemble des prestataires de services de confiance qualifiés.

I.2. Cadre juridique

Les services d'envoi recommandé électronique qualifiés, respectant les exigences spécifiées au chapitre II du présent document, bénéficient des effets juridiques définis à l'article 43 du règlement [eIDAS].

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.
CSPN	Certification de Sécurité de Premier Niveau.
PSCo	Prestataire de Services de Confiance.

II. Exigences relatives aux services d'envoi recommandé électronique qualifiés

II.1. Modalités de qualification

II.1.1. Processus de qualification

Le processus de qualification d'un service d'envoi recommandé électronique qualifié s'inscrit dans le processus de qualification du prestataire de services de confiance, tel que décrit dans la note [PSCO_QUALIF].

II.1.2. Considérations relatives à l'inscription dans la liste de confiance

Un service d'envoi recommandé électronique qualifié est identifié dans la liste de confiance :

- au moyen du certificat électronique utilisé pour apposer le cachet permettant de sécuriser l'envoi et la réception des données ; ou
- au moyen du certificat électronique d'une autorité de certification opérée sous la responsabilité du PSCo qualifié, uniquement pour ses propres besoins, et ne délivrant pas de certificats pour des services d'envoi recommandé électronique non qualifiés.

Dans le premier cas, si plusieurs certificats de cachet électronique sont mis en œuvre pour un même service d'envoi recommandé électronique qualifié, cela donne lieu à l'inscription de plusieurs services dans la liste de confiance.

Dans le second cas, l'évaluation de la conformité doit permettre de démontrer que cette autorité de certification ne délivre des certificats qu'à l'attention exclusive de services de confiance opérés par le PSCo qualifié, et que celui-ci a mis en place des mesures organisationnelles et techniques appropriées afin d'assurer qu'aucun des certificats délivrés n'est utilisé par un service d'envoi recommandé électronique non qualifié.

II.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences applicables du règlement [eIDAS] aux services d'envoi recommandé électronique qualifié, spécifiées dans les articles suivants :

- 24(2).e Utilisation de systèmes et produits fiables, sécurité et fiabilité des processus ;
- 24(2).h Conservation des informations délivrées et reçues dans le cadre d'envoi recommandé électronique ;
- 24(2).i Continuité de service suite à l'arrêt d'activité d'envoi recommandé électronique ;
- 44(1).a Fourniture des services par un ou plusieurs prestataires de services de confiance qualifiés ;
- 44(1).b Identification de l'expéditeur avec un degré de confiance élevé ;
- 44(1).c Identification du destinataire avant la fourniture des données ;
- 44(1).d : Sécurisation de l'envoi et la réception des données par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié de manière à exclure toute possibilité de modification indétectable des données ;
- 44(1).e : Signalement à l'expéditeur et au destinataire des données de toute modification des données nécessaire pour l'envoi ou la réception de celles-ci ;
- 44(1).f : Indication de la date et l'heure d'envoi, de réception et de toute modification des données au moyen d'un horodatage électronique qualifié.

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des données et au plan d'arrêt d'activité, des exigences applicables[1] du standard [TS_102_640-3], et des compléments précisés dans le chapitre II.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

Note : Le service d'envoi recommandé électronique doit également correspondre à la définition du règlement [eIDAS], telle que précisée à l'article 3(36) :

« un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée. »

[1] Le standard [TS_102_640-3] traite de l'envoi de courriers électroniques recommandés, et référence des versions obsolètes de normes et standards. Les exigences de ce standard doivent être adaptées au contexte de l'envoi recommandé électronique qualifié, et à l'état de l'art de la normalisation.

II.3. Compléments aux normes [EN_319_401] et [TS_102_640-3]

II.3.1. Compléments relatifs aux preuves d'envoi et de réception

Conformément à l'article 3(36) du règlement [eIDAS], on entend par «service d'envoi recommandé électronique», un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Il est ainsi attendu qu'un service d'envoi recommandé électronique qualifié mette à disposition de l'expéditeur les preuves d'envoi et de réception, de manière automatisée, fiable et efficace.

Les conditions générales d'utilisation du service d'envoi recommandé électronique qualifié doivent préciser les modalités de mise à disposition de ces preuves.

II.3.2. Compléments relatifs à l'utilisation de systèmes et produits fiables

Les modules cryptographiques employés pour les opérations nécessaires au service d'envoi recommandé électronique qualifié, notamment les opérations de création de cachet électronique, ou d'horodatage électronique le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

II.3.3. Compléments relatifs à la conservation des informations délivrées et reçues

Les exigences de la clause 7.10 de la norme [EN_319_401] et de la clause 6.5 du standard [TS_102_640-3] s'appliquent.

Le prestataire de service d'envoi recommandé électronique qualifié doit conserver pendant une durée minimale de sept (7) ans après la date d'envoi et de réception des données toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le PSCo précise dans ses conditions générales d'utilisation la durée de conservation effectivement appliquée ainsi que les modalités de réversibilité et de portabilité.

Les données à conserver sont au moins :

- l'identité de l'expéditeur du recommandé électronique ;
- une preuve de validation de l'identité de l'expéditeur ;
- une référence au document faisant l'objet de la demande d'envoi recommandé électronique ;
- les jetons d'horodatage électronique qualifié correspondant à la date et heure d'envoi, de réception et de modification des données le cas échéant ;
- l'identité du destinataire du recommandé électronique ;
- une preuve de validation de l'identité du destinataire ;
- les données relatives à la sécurisation de l'envoi (cachets électroniques).

II.3.4. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences de la clause 7.12 de la norme [EN_319_401] s'appliquent.

II.3.5. **Compléments relatifs à la fourniture du service par des prestataires de services de confiance qualifiés**

Si le service est fourni par plusieurs prestataires de services de confiance qualifiés, l'expéditeur et le destinataire de l'envoi recommandé électronique doivent être informés de l'identité de l'ensemble des PSCo qualifiés contribuant au service.

Chaque PSCo doit s'assurer, sur une base régulière et au moyen des listes de confiance publiées par les Etats membres, du maintien de la qualification des PSCo partenaires.

II.3.6. **Compléments relatifs à l'identification de l'expéditeur**

II.3.6.1. Vérification initiale de l'identité de l'expéditeur

Le service d'envoi recommandé électronique qualifié doit garantir l'identification de l'expéditeur avec un degré de confiance élevé.

Pour la vérification d'identité de l'expéditeur, les exigences définies au chapitre II.3.1 du référentiel [eIDAS_DELIV_CERT] s'appliquent *mutatis mutandis* à l'envoi recommandé électronique.

II.3.6.2. Identification et authentification de l'expéditeur

Postérieurement à la vérification d'identité, le prestataire de service d'envoi recommandé électronique qualifié peut attribuer un moyen d'identification à l'expéditeur, qu'il pourra utiliser pour s'authentifier à chaque envoi.

Dans ce cas, les méthodes d'authentification décrites dans les points 6.3.b à 6.3.f du standard [TS_102_640-3] sont acceptables. La méthode décrite au point 6.3.a de ce standard n'est pas acceptable.

L'authentification doit être forte (via l'emploi de deux facteurs distincts), et le mécanisme d'authentification mis en œuvre doit être dynamique. Il est recommandé que le moyen d'identification fasse au minimum l'objet d'une Certification de Sécurité de Premier Niveau (CSPN).

Le moyen d'authentification doit être sous le contrôle exclusif de l'utilisateur, et mettre en œuvre des contrôles de sécurité de sorte qu'il soit hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.

Dans le cas où le moyen d'identification repose sur l'utilisation un certificat de signature ou de cachet électronique, il est recommandé que ce certificat soit qualifié.

Note : Ce moyen d'identification peut être délivré par un autre organisme que le prestataire de services d'envoi recommandé électronique qualifié.

Si le PSCo n'attribue pas de moyen d'identification à l'expéditeur, la vérification d'identité doit être réalisée à chaque envoi dans les conditions décrites au chapitre II.3.6.1 ci-dessus.

II.3.7. **Compléments relatifs à l'identification du destinataire**

II.3.7.1. Vérification initiale de l'identité du destinataire

Le service d'envoi recommandé électronique qualifié doit garantir l'identification du destinataire avant la fourniture des données.

Pour la vérification d'identité du destinataire, il est recommandé lorsque cela est possible d'appliquer les mêmes exigences que pour l'identification de l'expéditeur. A défaut, cette vérification d'identité doit au minimum respecter les exigences du chapitre 2.1 du règlement [RE_2015_1502] pour le niveau substantiel.

II.3.7.2. Identification et authentification du destinataire

Postérieurement à la vérification d'identité, le prestataire de service d'envoi recommandé électronique qualifié peut attribuer un moyen d'identification au destinataire, qu'il pourra utiliser pour s'authentifier à chaque réception.

Les exigences et recommandations applicables au moyen d'identification de l'expéditeur sont applicables au moyen d'identification du destinataire.

Note : Ce moyen d'identification peut être délivré par un autre organisme que le prestataire de services d'envoi recommandé électronique qualifié.

Si le PSCo n'attribue pas de moyen d'identification au destinataire, la vérification d'identité doit être réalisée à chaque réception dans les conditions décrites au chapitre II.3.7.1 ci-dessus.

II.3.8. **Compléments relatifs à la sécurisation des envois et réceptions par un cachet électronique**

Les exigences définies à la clause 6.4 du standard [TS_102_640-3] s'appliquent.

Les modules cryptographiques employés pour apposer le cachet électronique avancé sécurisant l'envoi et la réception des données doivent être conformes aux règles définies dans la note [PSCO_QUALIF].

Il est recommandé que le certificat sur lequel repose ce cachet électronique soit un certificat qualifié au titre du règlement eIDAS.

Si le cachet électronique avancé est apposé par un prestataire de services de confiance qualifié distinct du prestataire de services d'envoi recommandé électronique qualifié, ce dernier doit vérifier la validité de ce cachet.

Note : Le règlement [eIDAS] prévoit que l'envoi et la réception puissent être sécurisés au moyen d'une signature électronique avancée ou d'un cachet électronique avancé du PSCo qualifié. Pour autant, en France, les PSCo qualifiés étant nécessairement des personnes morales, seule la sécurisation par le biais d'un cachet électronique avancé devrait être mise en œuvre.

II.3.9. **Compléments relatifs au signalement des modifications de données**

Le service d'envoi recommandé électronique qualifié doit signaler clairement toute modification des données nécessaire pour l'envoi ou la réception de celles-ci à l'expéditeur et au destinataire des données

Le PSCo précise dans ses conditions générales d'utilisation les moyens utilisés pour le signalement de ces modifications.

II.3.10. **Compléments relatifs à l'horodatage électronique qualifié**

La date et l'heure d'envoi, de réception et toute modification des données doivent être indiquées par un horodatage électronique qualifié.

Le prestataire de service d'envoi recommandé électronique qualifié peut s'appuyer sur un prestataire de service d'horodatage qualifié tiers pour réaliser cette opération. Dans ce cas, la validité du jeton d'horodatage électronique qualifié doit être systématiquement vérifiée.

Annexes

I. Annexe 1 Références documentaires

Renvoi	Document
[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 http://www.ssi.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
[NOTIFICATION]	Note des autorités française du 17 février 2015 à la Commission, désignant l'ANSSI comme organe de contrôle au titre du règlement eIDAS.
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur http://www.ssi.gouv.fr
[TS_102_640-3]	ETSI TS 102 640-3 V2.1.2 (2011-09) : Technical Specification Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains

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

Article	Exigence du règlement eIDAS	Clauses applicables des normes européennes	Chapitres applicables du présent document
3(36)	Définition de l'envoi recommandé électronique	*Non couvert*	II.3.1
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_401] Clause 7.7 [TS_102_640-3] Clause 6.4.3	II.3.2
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance	[EN_319_401] Clause 7.10 [TS_102_640-3] Clause 6.5	II.3.3
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_401] Clause 7.12	II.3.4
44(1).a	44(1).a Les services sont fournis par un ou plusieurs prestataires de services de confiance qualifiés	*Non couvert*	II.3.5
44(1).b	Le service doit garantir l'identification de l'expéditeur avec un degré de confiance élevé	[TS_102_640-3] Clause 6.3	II.3.6
44(1).c	Le service doit garantir l'identification du destinataire avant la fourniture des données	[TS_102_640-3] Clause 6.3	II.3.7
44(1).d	L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié de manière à exclure toute possibilité de modification indétectable des données	[TS_102_640-3] Clause 6.4	II.3.8
44(1).e	Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données	*Non couvert*	II.3.9
44(1).f	La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.	*Non couvert*	II.3.10