Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

**Premier ministre**

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

# Services de délivrance des 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 1.1 du 3 janvier 2017*

| HISTORIQUE DES VERSIONS | | | |
|---|---|---|---|
| **DATE** | **VERSION** | **EVOLUTION DU DOCUMENT** | **REDACTEUR** |
| 20/06/2016 | 1.0 | Version pour application au 1er juillet 2016. | ANSSI |
| 03/01/2017 | 1.1 | Version pour application au 31 janvier 2017.<br>*Modifications :*<br>- *Précisions relatives au maintien du statut qualifié et à l'inscription dans la liste de confiance ;*<br>- *Rappel des critères d'évaluation de la conformité ;*<br>- *Amendement des recommandations relatives à la fourniture du statut de révocation des certificats au-delà de leur période de validité, en accord avec l'évolution des normes ;*<br>- *Précisions et corrections relatives aux profils de certificats recommandés ;*<br>- *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 les services de confiance qualifiés qu'ils fournissent.

La présente note décrit les modalités de transition de la qualification [RGS] vers [eIDAS] des services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet.

## I.2. Cadre juridique

Les certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet délivrés par un prestataire de services de confiance respectant les exigences spécifiées au chapitre II du présent document sont présumés satisfaire aux exigences, respectivement, de l'annexe I, de l'annexe III et de l'annexe IV du règlement [eIDAS].

Les signatures électroniques avancées, reposant sur un certificat qualifié, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article 25 du règlement [eIDAS].

Les cachets électroniques avancés, reposant sur un certificat qualifié, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article 35 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. |
| **PSCE** | Prestataire de Services de Certification Electronique. |
| **RGS** | Référentiel Général de Sécurité. |
| **LCR** | Liste des Certificats Révoqués. |
| **OCSP** | *Online Certificate Status Protocol*. |

# II. Exigences relatives aux services de délivrance de certificats qualifiés

## II.1. Modalités de qualification

### II.1.1. Processus de qualification

Les modalités de qualification décrites ci-après sont applicables aux services de délivrance de certificats ayant déjà fait l'objet d'une qualification selon le [RGS], préalablement à la demande de qualification selon le règlement [eIDAS].

Un service de délivrance de certificats, qualifié selon le [RGS], peut prétendre à la qualification selon le règlement [eIDAS] aux conditions suivantes :

1. l'offre de délivrance de certificats est qualifiée selon le [RGS] au niveau 2 étoiles (**) ou 3 étoiles (***) ; et
2. le rapport d'évaluation sur la base duquel la décision de qualification [RGS] pour le niveau 2 étoiles (**) ou 3 étoiles (***) a été prononcée par l'organisme de qualification est transmis à l'ANSSI ; et
3. la conformité à l'ensemble des exigences supplémentaires définies dans le règlement [eIDAS] et rappelées au chapitre II.3 de la présente note est évaluée par un organisme d'évaluation respectant les critères de reconnaissance des organismes d'évaluation de la conformité des prestataires de service de confiance établis dans [CRITERES_OEC]. Cet organisme d'évaluation peut être distinct de celui qui a octroyé la qualification [RGS] ; et
4. le rapport d'évaluation de la conformité du PSCE aux exigences supplémentaires du règlement [eIDAS] rappelées au chapitre II.3 de la présente note est transmis à l'ANSSI.

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

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

La qualification [eIDAS] est octroyée par l'ANSSI au maximum jusqu'à la date de fin de validité de la qualification [RGS] sans toutefois excéder 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

Un service de délivrance de certificats qualifiés est identifié dans la liste de confiance, conformément à la clause 5.5.3 du standard [TS_119_612], au moyen du certificat électronique d'une autorité de certification racine, intermédiaire ou terminale.

Il est attendu que la valeur de l'attribut « *Organization* », figurant dans le certificat d'autorité de certification 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.

Note : L'évaluation de la conformité doit permettre de démontrer que, sous cette autorité de certification, il est possible de distinguer sans ambiguïté les certificats qualifiés et non qualifiés délivrés par celle-ci. En particulier, il est nécessaire de s'assurer que les certificats non qualifiés ne comportent pas d'attributs pouvant les faire considérer de manière erronée comme des certificats qualifiés.

Il est possible d'assortir cette identification de contraintes supplémentaires permettant d'identifier les certificats qualifiés délivrés sous cette autorité (*par exemple, au moyen d'un OID de politique de certification).*

Dans ce cas, l'évaluation de la conformité devra couvrir un périmètre cohérent avec les contraintes supplémentaires positionnées dans la liste de confiance (*par exemple, cette évaluation devra couvrir l'ensemble du périmètre relatif à un OID de politique de certification donné, et vérifier que cet OID n'est pas renseigné dans des certificats non qualifiés).*

Note : Afin de réduire le périmètre audité, il est recommandé d'identifier le service au moyen d'une autorité de certification terminale, délivrant uniquement des certificats qualifiés.

L'inscription, dans la liste de confiance, d'un nouvel élément d'identification pour un service précédemment qualifié (*par exemple, l'ajout d'un nouveau certificat électronique 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 aux services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, spécifiées dans les articles suivants :

- Pour les prestataires de services de confiance qualifiés délivrant des certificats qualifiés :
    - 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(1) Vérification de l'identité et des attributs spécifiques de la personne physique ou morale ;
    - 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 ;
        - h Conservation des informations délivrées et reçues dans le cadre de la délivrance des certificats qualifiés ;
        - i Continuité de service suite à l'arrêt d'activité de délivrance de certificats qualifiés ;
        - j Traitement licite des données à caractère personnel ;
        - k Base de données relative aux certificats émis ;
    - 24(3) Révocation des certificats ;
    - 24(4) Accès fiable, gratuit et efficace au statut de révocation des certificats.
- Pour les certificats qualifiés :
    - 28(1) Profils des certificats qualifiés de signature électronique ;
    - 28(3) Autorisation d'attributs spécifiques complémentaires non obligatoires ;
    - 28(4) Aspect relatifs à la révocation de ces certificats ;
    - 28(5) Aspects relatifs à la suspension de ces certificats ;
    - 38(1), (3), (4), (5) Profils des certificats qualifiés de cachet électronique, aspects relatifs à la révocation et suspension de ces certificats ;
    - 45(1) Profils des certificats qualifiés d'authentification de site Internet.

Le respect des exigences du [RGS] applicables aux services de délivrance de certificats qualifiés au niveau 2 étoiles (**) ou 3 étoiles (***) et des compléments précisés dans le chapitre II.3 du présent document permet d'apporter une présomption de conformité à ces exigences.

## II.3. Compléments au [RGS]

### II.3.1. Compléments relatifs à l'accessibilité aux personnes handicapées

Dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services, sont accessibles aux personnes handicapées.

### II.3.2. Compléments relatifs à la gestion des risques

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

Le PSCE 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 risques et la décision d'homologation doivent être jointes au rapport d'évaluation de la conformité transmis lors de la demande de qualification.

### II.3.3. Compléments relatifs à l'information de l'organe de contrôle

Le PSCE doit prévenir l'ANSSI en cas de changement ou cessation d'activité.

Le PSCE doit également 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.3.4. Compléments relatifs à la vérification de l'identité du demandeur

La vérification de l'identité de la personne physique, ou du représentant autorisé de la personne morale, à laquelle le prestataire de service de confiance délivre un certificat qualifié peut être réalisée, conformément aux règles du RGS pour le niveau deux étoiles (**), soit :

1. lors d'un face à face, en présence physique de la personne ; ou
2. sous forme dématérialisée à condition que la demande soit signée à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau deux étoiles (**) décrites dans le document [RGS_A1], que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS[1].

[1] En vertu de l'article 51 du règlement [eIDAS], et sous réserve du respect des délais de transition prévus dans ledit article, les certificats qualifiés selon le [RGS] au niveau 3 étoiles ou qualifiés au titre de l'arrêté du 26 juillet 2004 sont considérés comme des certificats qualifiés au titre du règlement [eIDAS].

### II.3.5. Compléments relatifs au statut de révocation des certificats

Le PSCE doit assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

Afin de répondre à cette exigence, il est recommandé d'appliquer les règles suivantes, selon le cas :

1) Après l'expiration du certificat qualifié :
    a. si le PSCE assure la publication d'une LCR, celle-ci devrait :
        i. comporter l'extension « *ExpiredCertsOnCRL* », comme prévu par la recommandation ITU-T X.509 ; et
        ii. contenir les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.
    b. si le PSCE met en œuvre un répondeur OCSP, celui-ci devrait :
        i. comporter l'extension « *archive cutoff* », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC ; et
        ii. maintenir disponible le statut de révocation du certificat après son expiration.

2) Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer :
    a. l'ensemble des certificats non-expirés émis par cette AC devraient être révoqués ; et
    b. si le PSCE assurait la publication d'une LCR, une dernière LCR devrait être publiée, celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »); et
    c. si le PSCE assurait un service de répondeur OCSP, une dernière réponse OCSP devrait être pré-générée pour chaque certificat émis, cette réponse ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »).

3) Lorsque le PSCE cesse de fournir le service de confiance qualifié, sans le transférer vers un autre PSCE qualifié :
    a. les méthodes applicables au cas n°2 sont applicables dans ce cas. En complément, le PSCE n'est pas tenu de maintenir la publication des LCR ni de maintenir le service OCSP, mais les LCR et/ou réponses OCSP produites devraient être mises à disposition des clients du PSCE dans des conditions permettant de garantir leur intégrité.

Dans tous les cas, le PSCE doit rendre publique les mesures mises en œuvre pour répondre à l'exigence.

### II.3.6. Compléments relatifs aux profils des certificats

Les exigences suivantes s'appliquent aux profils de certificats en complément de celles du RGS :

- l'extension « *QCStatements* » doit être valorisée de manière à indiquer, au moins sous une forme adaptée au traitement automatisé[2], que :
    - le certificat a été délivré comme certificat qualifié de signature électronique, de cachet électronique ou d'authentification de site internet ; et
    - le cas échéant, les données de création de signature ou de cachet électronique, associées aux données de validation de la signature ou du cachet électronique, se trouvent dans un dispositif de création de signature ou de cachet électronique qualifié ; et

Note : Pour les services délivrant des certificats qui ne bénéficient pas des mesures de transition de l'article 51 du règlement [eIDAS], l'extension « *QCStatements* » doit être valorisée conformément aux prescriptions du présent chapitre une fois que le statut qualifié est attribué au service dans la liste de confiance.

- le chemin d'accès vers le lieu de publication du certificat de l'AC doit être renseigné dans le certificat lui-même, par le biais de l'extension « *AuthorityInformationAccess* » ; et

- le champ « *SubjectDN* » d'un certificat qualifié d'authentification de site internet doit préciser la ville (*localityName*) ainsi que la région ou l'état (*StateorProvinceName*) où est établie la personne physique ou morale à laquelle le certificat a été délivré.

[2] la norme [EN_319_412-5] définit les règles permettant d'indiquer ces deux informations dans les certificats qualifiés de manière interopérable.

# Annexes

## I. Références documentaires

| Renvoi | Document |
|---|---|
| [CRITERES_OEC] | Organismes d'évaluation de la conformité – Critères de reconnaissance au titre du règlement eIDAS, version en vigueur.<br>Disponible sur http://www.ssi.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.<br>Disponible sur http://www.europa.eu |
| [EN_319_412-5] | ETSI EN 319 412-5 V2.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Certificate Profiles;<br>Part 5: QCStatements |
| [HOMOLOGATION] | L'homologation de sécurité en neuf étapes simples, version en vigueur<br>Disponible sur http://www.ssi.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. |
| [QUALIF_SERV] | Processus de qualification d'un service, version en vigueur.<br>Disponible sur http://www.ssi.gouv.fr |
| [RGS] | Référentiel général de sécurité, version 1 ou 2.<br>Disponible sur http://www.ssi.gouv.fr |
| [RGS_A1] | Annexe A1 au RGSv2.0 : Règles relatives à la mise en oeuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques. |
| [RGS_A2] | Annexe A2 au RGSv2.0 : Politique de Certification Type – certificats électroniques de personne |
| [RGS_A3] | Annexe A3 au RGSv2.0 : Politique de Certification Type – certificats électroniques de services applicatifs |
| [RGS_A4] | Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques |
| [TS_119_612] | ETSI TS 119 612 v2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI); Trusted Lists |

# II. Couverture des exigences spécifiques du règlement [eIDAS] par le [RGS]

| Article | Exigence du règlement eIDAS | Chapitres applicables du [RGS] | Chapitres applicables du présent document |
|---|---|---|---|
| 5(1) | Protection et traitement des données à caractère personnel | [RGS_A2] IX.4<br>[RGS_A3] IX.4 | *Pas de complément au RGS* |
| 13(2) | Limitation de responsabilités | [RGS_A2] II.2<br>[RGS_A3] II.2 | *Pas de complément au RGS* |
| 15 | Accessibilité | [RGS_A2] I.4.1<br>[RGS_A3] I.4.1 | Chapitre II.3.1 |
| 19(1) | Gestion des risques | [RGS_A2] I.4.1<br>[RGS_A3] I.4.1 | Chapitre II.3.2 |
| 19(2) | Notification des incidents | *Non couvert par le RGS* | Chapitre II.3.3 |
| 24(1) | Vérifications de l'identité du demandeur | [RGS_A2] III<br>[RGS_A3] III | Chapitre II.3.4 |
| 24(2).a | Information de l'organe de contrôle relative aux modifications des services | *Non couvert par le RGS* | Chapitre II.3.3 |
| 24(2).b | Expertise, fiabilité, expérience et qualification des personnels et sous-traitants | [RGS_A2] V.3<br>[RGS_A3] V.3 | *Pas de complément au RGS* |
| 24(2).c | Maintien de ressources financières suffisantes et/ou assurance responsabilité | [RGS_A2] IX.2<br>[RGS_A3] IX.2 | *Pas de complément au RGS* |
| 24(2).d | Information des conditions et limites d'utilisation des services | [RGS_A2] II.2<br>[RGS_A3] II.2 | *Pas de complément au RGS* |
| 24(2).e | Utilisation de systèmes et produits fiables | [RGS_A2] VI.2 et VI.3<br>[RGS_A3] VI.2 et VI.3 | *Pas de complément au RGS* |
| 24(2).f | Utilisation de systèmes fiables pour le stockage des données | [RGS_A2] VI.5 et VI.6<br>[RGS_A3] VI.5 et VI.6 | *Pas de complément au RGS* |
| 24(2).g | Mesures contre la falsification et le vol des données | [RGS_A2] V<br>[RGS_A3] V | *Pas de complément au RGS* |
| 24(2).h | Conservation des informations délivrées et reçues par le prestataire de services de confiance | [RGS_A2] V.4<br>[RGS_A3] V.4 | *Pas de complément au RGS* |
| 24(2).i | Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance | [RGS_A2] V.7 et V.8<br>[RGS_A3] V.7 et V.8 | *Pas de complément au RGS* |
| 24(2).j | Traitement licite des données à caractère personnel | [RGS_A2] IX.4<br>[RGS_A3] IX.4 | *Pas de complément au RGS* |
| 24(3) | Révocation des certificats | [RGS_A2] IV.9.5.2<br>[RGS_A3] IV.9.5.2. | *Pas de complément au RGS* |
| 24(4) | Accès automatisé, disponible à tout moment, fiable, gratuit et efficace au statut de révocation du certificat | [RGS_A2] IV.10.2<br>[RGS_A3] IV.10.2 | Chapitre II.3.5 |
| 28(1) | Certificats qualifiés de signature électronique | [RGS_A4] II.2 | Chapitre II.3.6 |
| 38(1) | Certificats qualifiés de cachet électronique | [RGS_A4] II.3 | Chapitre II.3.6 |

| Article | Exigence du règlement eIDAS | Chapitres applicables du [RGS] | Chapitres applicables du présent document |
|---|---|---|---|
| 45(1) | Certificats qualifiés d'authentification de site internet | [RGS_A4] II.3 | Chapitre II.3.6 |
| 28(4)<br>38(4) | Aspect relatifs à la révocation | [RGS_A2] IV.9<br>[RGS_A3] IV.9 | Chapitre II.3.5 |
| 28(5)<br>38(5) | Aspects relatifs à la suspension | [RGS_A2] IV.9<br>[RGS_A3] IV.9 | *Pas de complément au RGS* |