Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Règlement eIDAS

Foire aux questions

Version 1.0 du 2 juin 2016

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
02/06/2016	1.0	Version pour publication	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. Questions générales sur le règlement eIDAS

I.1. Qu'est-ce que le règlement eIDAS ?

Le règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS », est un règlement européen qui a été adopté le 23 juillet 2014 par le Parlement européen et le Conseil de l'Union Européenne. L'objectif de ce règlement est de mettre en place un cadre juridique propre à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur.

I.2. Quels sont les sujets couverts par le règlement eIDAS ?

Le règlement eIDAS s'applique à l'identification électronique et aux services de confiance (faisant respectivement l'objet des chapitres II et III du présent document). Il accorde également un effet juridique aux documents électroniques.

I.3. Quand le règlement eIDAS a-t-il été publié ? Quand est-il entré en vigueur et quand devient-il applicable ?

Le règlement eIDAS a été publié au Journal Officiel de l'Union Européenne (JOUE) le 28 août 2014. Il est entré en vigueur le 17 septembre 2014.

Le règlement devient applicable :

- le **29 septembre 2015** pour la notification et la reconnaissance volontaire des moyens d'identification électronique par les Etats membres ;
- le **29 septembre 2018** pour la reconnaissance mutuelle obligatoire des moyens d'identification électronique par les Etats membres ;
- le **1er juillet 2016** pour les services de confiance et les documents électroniques.

I.4. Qui est concerné par le règlement eIDAS ?

Le règlement concerne les citoyens, les entreprises, les organismes du secteur public et les prestataires de services de confiance établis dans l'Union européenne. Il couvre en particulier les échanges entre usagers et administrations.

Les mécanismes de reconnaissance mutuelle des moyens d'identification électroniques et des signatures électroniques, détaillés dans les chapitres II et IV du présent document, s'appliquent ainsi uniquement aux administrations dans leurs relations avec les usagers.

En revanche, le règlement ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés n'ayant pas d'impact direct sur des tiers, résultant du droit national ou d'accords au sein d'un ensemble défini de participants. *Par exemple, une autorité administrative mettant en œuvre une infrastructure de gestion de clés pour couvrir ses besoins internes ne serait pas soumise aux exigences du règlement eIDAS applicables aux services de confiance.*

I.5. Le règlement eIDAS s'applique-t-il uniquement aux échanges transfrontières ?

Le règlement eIDAS ne s'applique pas uniquement aux échanges transfrontières. En effet, si les aspects transnationaux sont au cœur du règlement eIDAS, notamment via les mécanismes de reconnaissance mutuelle des moyens d'identification électronique et des services de confiance, le règlement a la vocation plus globale d'instaurer un climat de confiance dans l'environnement en ligne, y compris au niveau national.

I.6. Que sont les actes délégués et actes d'exécution du règlement eIDAS ?

Les actes délégués et actes d'exécution constituent la « législation secondaire » du règlement eIDAS. Ce sont des actes prévus par des articles du règlement, venant préciser les modalités d'application de ces derniers.

Ces actes peuvent notamment être utilisés afin de référencer des normes permettant d'apporter une présomption de conformité aux exigences du règlement, et harmoniser ainsi les pratiques au sein des différents Etats membres.

Certains de ces actes sont obligatoires pour permettre la mise en application du règlement, mais la majorité est optionnelle.

A ce jour, aucun acte délégué n'a été publié. Seuls les sept actes d'exécution obligatoires, et un acte d'exécution optionnel, ont été publiés. Ceux-ci sont référencés dans les chapitres II et III du présent document.

I.7. Quels sont les impacts et caractéristiques du règlement eIDAS sur le plan juridique ?

En dehors de ses effets particuliers concernant l'identification électronique et les services de confiance, qui sont détaillés dans la suite de la présente FAQ, le règlement a les impacts suivant :

- il abroge la directive 1999/93/EC sur la signature électronique ;
- il accorde un effet juridique aux documents électroniques, précisant qu'ils ne peuvent être refusés comme preuve en justice au seul motif qu'ils se présentent sous forme électronique.

De plus, s'agissant d'un règlement, il est d'application directe, ce qui signifie qu'il ne nécessite pas de transposition en droit national et que toute disposition nationale allant à l'encontre des dispositions du règlement est considérée comme non applicable.

I.8. Quel est le rôle de l'ANSSI au titre du règlement eIDAS ?

L'ANSSI intervient à plusieurs titres dans l'application du règlement eIDAS : en tant que garante de la sécurité pour son volet « identification électronique », en tant qu'organe de contrôle pour son volet « services de confiance », en tant qu'organisme de certification des dispositifs de création de signature ou de cachet qualifiés, et enfin en tant qu'organisme en charge de la liste de confiance.

Ces responsabilités sont détaillées dans les chapitres II et III du présent document.

II. Questions relatives à l'identification électronique

II.1. Quel est l'objectif du volet « identification électronique » du règlement eIDAS ?

L'objectif du règlement eIDAS pour l'identification électronique est de mettre en place un cadre d'interopérabilité pour les identités électroniques des différents Etats membres. Le règlement :

- Définit les spécifications permettant l'**interopérabilité** des moyens d'identification électroniques ;
- Définit les **niveaux de garantie**, et exigences de sécurité associées, de ces moyens ;
- Précise les conditions de **reconnaissance mutuelle** des moyens d'identification électroniques délivrés dans les Etats membres.

II.2. Quels sont les principes du volet « identification électronique » du règlement eIDAS ?

Le règlement instaure un système de notification de « schémas d'identification électronique » par les Etats membres. Ces derniers sont définis par le règlement comme des *« systèmes pour l'identification électronique, en vertu desquels des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales »*. Au sens du règlement, un moyen d'identification électronique est *« un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier sur un service en ligne »*.

Le règlement prévoit trois niveaux de garantie pour les moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié : faible, substantiel et élevé. Le règlement d'exécution n° 2015/1502 du 8 septembre 2015 fixe les spécifications de sécurité minimales pour chacun de ces niveaux.

II.3. Quels sont les actes d'exécution publiés au titre du chapitre « identification électronique » du règlement ?

Les actes d'exécution relatifs à l'identification électronique publiés à la date de rédaction du présent document sont les suivants :

- Décision d'exécution n° **2015/296** du 24 février 2015 établissant les **modalités de coopération entre les États membres** en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement n° 910/2014 ;
- Règlement d'exécution n° **2015/1501** du 8 septembre 2015 sur le **cadre d'interopérabilité** visé à l'article 12, paragraphe 8, du règlement n° 910/2014 ;
- Règlement d'exécution n° **2015/1502** du 8 septembre 2015 fixant les **spécifications techniques et procédures minimales relatives aux niveaux de garantie** des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement n° 910/2014 ;
- Décision d'exécution n° **2015/1984** du 3 novembre 2015 définissant **les circonstances, les formats et les procédures pour les notifications** visés à l'article 9, paragraphe 5, du règlement n° 910/2014.

II.4. Quelles sont les conditions préalables à la notification d'un schéma d'identification électronique par un Etat membre ?

Le règlement eIDAS n'oblige pas les Etats membres à mettre en œuvre un moyen d'identification électronique au niveau national ni, le cas échéant, à le notifier à la Commission européenne.

Le cas échéant, un Etat membre souhaitant notifier un schéma d'identification électronique doit au préalable :

- permettre l'utilisation du moyen d'identification électronique délivré dans le cadre de ce schéma pour accéder à au moins un service en ligne fourni par un organisme du secteur public de l'Etat membre notifiant ;
- fournir la description du schéma aux autres Etats membres six mois au moins avant la notification.

II.5. Quelles sont les obligations d'un Etat membre notifiant un schéma d'identification électronique ?

Si un Etat membre choisit de notifier un schéma d'identification électronique, cela génère pour lui les obligations suivantes :

- **respecter les spécifications de sécurité minimales** définies dans le règlement d'exécution n°2015/1502 du 8 septembre 2015 ainsi que les spécifications d'interopérabilité définies dans l'acte d'exécution n°2015/1501 du 8 septembre 2015 ;
- **fournir une authentification en ligne** afin de permettre à toute partie utilisatrice établie sur le territoire d'un autre Etat membre de confirmer les données d'identification personnelle reçues sous forme électronique ;
- **suspendre ou révoquer l'authentification transfrontalière** en cas d'atteinte à la sécurité du schéma d'identification électronique, et notifier son retrait s'il ne peut être remédié à l'atteinte dans un délai de trois mois.

L'Etat membre notifiant est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement à ces obligations, dans le cas d'une authentification transfrontalière.

II.6. Les organismes du secteur public sont-ils tenus de recourir à des moyens d'identification électronique au sens du règlement eIDAS ?

Le règlement eIDAS n'oblige pas les organismes du secteur public des différents Etats membres à recourir à des moyens d'identification électronique délivrés dans le cadre de schémas d'identification électroniques notifiés. *Par exemple, les administrations ayant mis en œuvre des authentifications reposant sur des certificats électroniques pour l'accès à leurs téléservices, ne sont pas tenues de les faire évoluer.*

Les organismes du secteur public peuvent toutefois, soit en vertu de pratiques administratives nationales, ou en vertu du droit national, exiger la mise en œuvre d'un moyen d'identification électronique pour l'accès à leurs téléservices.

II.7. Quelles obligations s'appliquent à un organisme du secteur public s'il exige le recours à un moyen d'identification électronique « eIDAS » pour l'accès à ses services ?

Si, dans un Etat membre, un organisme du secteur public exige, pour l'accès à l'un de ses services en ligne, une authentification reposant sur un moyen d'identification électronique de niveau de garantie substantiel ou élevé, il devra également accepter, pour l'accès à ce téléservice, l'ensemble des moyens d'identification électronique de niveau équivalent ou supérieur et relevant d'un schéma d'identification notifié à la Commission et publié au JOUE. Cette obligation sera effective à compter du **29 septembre 2018**.

Par ailleurs, les organismes du secteur public peuvent décider, sur une base volontaire, de reconnaître les schémas d'identification électronique de niveau faible, ainsi que les schémas d'identification électronique notifiés avant le 29 septembre 2018.

II.8. Quelles sont les conditions d'obtention d'un moyen d'identification électronique ?

Les moyens d'identification électronique peuvent être demandés par des personnes physiques ou morales, ou par des personnes physiques représentant des personnes morales.

Pour obtenir un moyen d'identification électronique, le demandeur doit pouvoir justifier de son identité dans les conditions prévues par le règlement d'exécution n° 2015/1502, qui précise en annexe les exigences minimales relatives à la vérification d'identité des personnes physiques et à la délivrance du moyen d'identification.

Ces exigences peuvent être renforcées par la réglementation nationale ou les pratiques du fournisseur d'identité, en fonction du niveau de garantie visé.

II.9. Un face à face est-il nécessaire pour obtenir un moyen d'identification électronique ?

Le règlement d'exécution n°2015/1502 précise uniquement, selon le niveau de garantie, la nature des vérifications devant être réalisées (authenticité des pièces d'identité présentées, comparaison de caractéristiques physiques du demandeur…) sans spécifier le moyen technique ou organisationnel.

En particulier, le face à face (c'est-à-dire une rencontre en personne entre le demandeur de l'identification et la personne délivrant le moyen d'identification) n'est pas exigé. Par conséquent, l'existence d'un face à face dans la procédure de vérification d'identité et/ou dans celle de délivrance du moyen d'identification électronique dépendra des choix techniques effectués par l'organisme délivrant ce moyen.

II.10. Comment se déroule la mise en œuvre au niveau national du volet « identification électronique » du règlement eIDAS ?

La Direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC) assure le rôle d'autorité nationale en matière d'identification électronique. A ce titre, elle :

- est le point de contact unique de la Commission ;
- est responsable de la notification des schémas d'identification électronique nationaux ;
- pilote la participation française au réseau de coopération prévu dans le cadre du règlement ;
- porte le programme FranceConnect, qui est le nœud assurant l'interopérabilité avec les indentifications électroniques et fournisseurs de service des autres Etats membres ;
- vérifie le respect des exigences d'interopérabilité et assure le raccordement des fournisseurs d'identité à FranceConnect.

L'ANSSI est garante de la sécurité pour le volet identification électronique du règlement eIDAS. A ce titre, elle :

- établit le référentiel des exigences de sécurité applicables à chaque niveau de garantie des moyens d'identification électronique ;
- évalue le bon respect de ces exigences par les organismes fournissant les moyens d'identification électroniques.

III. Questions relatives à l'ensemble des services de confiance

III.1. Quel est l'objectif du volet « services de confiance » du règlement eIDAS ?

L'objectif du règlement est d'instaurer un cadre juridique général pour l'utilisation des services de confiance. Il étend le champ d'application de la directive 1999/93/CE au-delà de la seule signature électronique et englobe les services de :

- création, vérification et validation de signatures électroniques, de cachets électroniques, d'horodatage électronique, d'envoi recommandé électronique et de certificats relatifs à ces services ;
- création, vérification et validation de certificats pour l'authentification de sites internet ;
- conservation de signatures électroniques et de cachets électroniques ou des certificats relatifs à ces services.

III.2. Quels sont les principes du volet « services de confiance » du règlement eIDAS ?

Le règlement établit une distinction entre les services de confiance qualifiés et les services de confiance non qualifiés. Les services de confiance qualifiés peuvent bénéficier d'effets juridiques spécifiques précisés dans le règlement et sont assurés par des prestataires de services de confiance qualifiés.

Le règlement accorde également des effets juridiques spécifiques aux signatures électroniques qualifiées et aux cachets électroniques qualifiés.

Enfin, le règlement instaure, au niveau national, un régime de contrôle des prestataires de service de confiance, passant en particulier par la désignation d'un organe de contrôle par chaque Etat membre.

III.3. Quels sont les actes d'exécution publiés au titre du chapitre « services de confiance » du règlement ?

Les actes d'exécution relatifs aux services de confiance publiés à la date de rédaction de cette FAQ sont les suivants :

- Règlement d'exécution n° **2015/806** du 22 mai 2015 établissant les **spécifications relatives à la forme du label de confiance de l'Union** pour les services de confiance qualifiés ;
- Décision d'exécution n° **2015/1505** du 8 septembre 2015 établissant les **spécifications techniques et les formats relatifs aux listes de confiance** visées à l'article 22, paragraphe 5, du règlement n° 910/2014 ;
- Décision d'exécution n° **2015/1506** du 8 septembre 2015 établissant les **spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés** devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement n° 910/2014 ;
- Décision d'exécution n° **2016/650** du 25 avril 2016 établissant des **normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique** conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014.

III.4. Quels sont les effets juridiques prévus par le règlement eIDAS ?

Le règlement eIDAS établit que l'effet juridique et la recevabilité comme preuve en justice des signatures électroniques, des cachets électroniques, des horodatages électroniques, et des envois recommandés électroniques, ne peuvent être refusés au seul motif qu'ils se présentent sous forme électronique ou qu'ils ne soient pas qualifiés.

En complément, le règlement précise les effets juridiques suivants :

- **la signature électronique qualifiée** bénéficie d'un effet juridique équivalent à celui d'une signature manuscrite ;
- **le cachet électronique qualifié** bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié ;
- **l'horodatage électronique qualifié** bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure ;
- **l'envoi recommandé électronique qualifié** bénéficie d'une présomption relative à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié, à leur réception par le destinataire identifié et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées.

III.5. Quelles sont les exigences applicables aux prestataires de services de confiance ?

Le règlement formule des obligations à l'encontre de l'ensemble des prestataires de services de confiance, qu'ils soient qualifiés ou non. En particulier, ils doivent, sous peine de sanctions fixées par les Etats membres :

- effectuer le traitement de données à caractère personnel conformément à la directive 95/46/CE ;
- rendre accessible aux personnes handicapées, dans la mesure du possible, leurs services de confiance ainsi que les produits servant à fournir ces services et destinés à un utilisateur final ;
- prendre les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services qu'ils fournissent ;
- notifier à l'organe de contrôle (et, lorsque l'atteinte est susceptible de lui porter préjudice, la personne physique ou morale concernée) 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.

Les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement à leurs obligations. Il incombe à la partie invoquant ces dommages de prouver l'intention ou la négligence d'un prestataire de services de confiance non qualifié.

III.6. Quelles sont les obligations induites du volet « services de confiance » du règlement eIDAS pour les prestataires de services de confiance qualifiés ?

Un prestataire de services de confiance qualifié est un prestataire de services de confiance offrant au moins un service de confiance qualifié. Le règlement formule des exigences générales applicables à l'ensemble des prestataires de services de confiance qualifiés, ainsi que des exigences spécifiques à chaque service de confiance qualifié.

Un prestataire de services de confiance qualifié doit avoir fait l'objet d'une évaluation de la conformité aux exigences du règlement, avoir obtenu son statut qualifié de l'organe de contrôle désigné par l'Etat membre dans lequel il est établi, et être identifié sur la liste de confiance avant de pouvoir commencer à fournir des services qualifiés.

Les prestataires de services de confiance qualifiés sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement à leurs obligations. Il incombe aux prestataires de services de confiance qualifiés de prouver que ces dommages ont été causés sans intention ni négligence de leur part.

III.7. Quels sont les services de confiance qualifiés prévus par le règlement ?

Les services de confiance qualifiés prévus par le règlement sont les suivants :

- la délivrance de certificats électroniques qualifiés pour la signature électronique, le cachet électronique ou l'authentification de site internet ;
- l'horodatage électronique ;
- la validation de signatures ou de cachets électronique ;
- la conservation de signatures ou de cachets électroniques ;
- l'envoi recommandé électronique.

La création de signatures électroniques qualifiées « à distance » n'est pas considérée comme un service de confiance qualifié au sens du règlement eIDAS.

III.8. Quel est le régime de contrôle des prestataires de services de confiance?

Le régime de contrôle prévu par le règlement repose sur des organes de contrôles désignés par chaque Etat membre, ayant pour mission :

- Le contrôle a priori des prestataires de service de confiance qualifiés établis sur le territoire français ;
- La prise des mesures, a posteriori et si nécessaire, en ce qui concerne les prestataires de service de confiance non qualifiés établis sur le territoire de cet Etat membre, lorsque l'organe de contrôle est informé que ces derniers ou les services qu'ils fournissent ne satisfont pas aux exigences du règlement ;

Les prestataires de services de confiance non qualifiés ne font ainsi pas l'objet d'un contrôle a priori.

Pour délivrer les qualifications des prestataires de services de confiance, les organes de contrôle s'appuient sur les rapports établis par des organismes d'évaluation de la conformité accrédités conformément au règlement n° 765/2008/CE.

III.9. Quelles sont les modalités de contrôle spécifiques aux prestataires de services de confiance qualifiés ?

Les prestataires de services de confiance qualifiés doivent se soumettre à un audit effectué à leurs frais, au moins tous les vingt-quatre mois, par un organisme d'évaluation de la conformité.

Le rapport établi par l'organisme d'évaluation de la conformité, et le cas échéant des éléments complémentaires, sont transmis, dans un délai de trois jours ouvrables, à l'organe de contrôle de l'État membre dans lequel le prestataire est établi. L'organe de contrôle vérifie la conformité aux exigences du règlement du service de confiance fourni et prononce la décision de qualification.

En dehors de ces audits réguliers, l'organe de contrôle peut décider à tout moment de soumettre un prestataire de services de confiance qualifiés, à ses frais, à un audit ou peut demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité du prestataire.

Cette évaluation de la conformité vise à confirmer le respect des exigences du règlement eIDAS. Elle n'a pas pour objectif de confirmer le respect d'une norme ou d'un standard technique.

III.10. Qu'est-ce qu'une liste de confiance ?

Chaque Etat membre établit et maintient à jour une liste de confiance sur laquelle figurent les informations relatives aux prestataires de services de confiance qualifiés dont ils sont responsables ainsi qu'aux services de confiance qualifiés qu'ils fournissent. Des informations relatives aux prestataires et services de confiance non qualifiés peuvent également figurer sur cette liste.

III.11. Qu'est-ce le label de confiance de l'Union ?

Le label de confiance de l'Union pour les services de confiance qualifiés peut être utilisé par les prestataires de services de confiance qualifiés inscrits sur les listes de confiance, pour indiquer de manière claire, simple et reconnaissable les services de confiance qualifiés qu'ils fournissent.

L'utilisation de ce label est assortie de l'obligation de rendre disponible, sur le site internet du prestataire de services de confiance qualifié, un lien vers la liste de confiance concernée.

Les spécifications du label de confiance font l'objet du règlement d'exécution n° 2015/806.

III.12. Qu'est-ce que le « mandat 460 » ?

Le mandat 460 est une initiative de la Commission européenne visant à établir un cadre normatif d'interopérabilité favorisant le développement du marché unique numérique européen.

Deux organismes de standardisation, l'ETSI (*European Telecommunications Standards Institute)* et le CEN (Comité Européen de Normalisation), ont ainsi été mandatés pour élaborer des normes et standards relatifs aux services de confiance. Suite à la publication du règlement eIDAS, les travaux réalisés dans le cadre du mandat 460 ont été ré-orientés afin d'accompagner la mise en œuvre du règlement.

L'objectif des travaux actuels est d'établir les normes permettant d'apporter une présomption de conformité aux exigences du règlement, et pouvant être référencées par le règlement au travers des actes d'exécution qu'il prévoit.

Toutefois, la grande majorité de ces normes ne sont pas aujourd'hui référencées par le règlement, les actes d'exécution nécessaires n'ayant pas été adoptés.

III.13. Les organismes du secteur public sont-ils contraints d'avoir recours à des services de confiance qualifiés ?

Le règlement n'impose pas aux organismes du secteur public des différents Etats membres d'avoir recours à des services de confiance qualifiés. Il appartient au droit national de déterminer les exigences applicables au sein de chaque Etat membre.

Le règlement formule toutefois des obligations relatives aux organismes du secteur public exigeant ou mettant en œuvre des signatures électroniques avancées ou qualifiées. Ces obligations sont précisées au chapitre IV du présent document.

III.14. Comment se déroule la mise en œuvre au niveau national du volet « services de confiance » du règlement eIDAS ?

La mise en œuvre du volet « services de confiance » sur le plan national repose principalement sur l'ANSSI, qui est l'organe de contrôle désigné par la France pour les services de confiance.

A ce titre, l'ANSSI assure notamment les missions suivantes :

- le contrôle complet a priori et a posteriori des prestataires de services de confiance qualifiés ;
- le contrôle a posteriori et sur saisie des prestataires de service de confiance non-qualifiés ;
- l'attribution et le retrait du statut « qualifié » aux prestataires de services de confiance qui en font la demande ;
- la conduite d'audits ou la requête d'évaluation de la conformité des prestataires de services de confiance qualifiés par des organismes d'évaluation ;
- la définition des modalités techniques de respect des exigences du règlement eIDAS ;
- l'analyse des rapports d'évaluation de la conformité ;
- la coopération avec les autres autorités nationales et les organes de contrôle établis dans les autres Etats membres, et l'établissement d'un rapport annuel à la Commission sur ses principales activités.

En marge de son rôle d'organe de contrôle, l'ANSSI a aussi en charge :

- l'établissement et la publication de la liste de confiance française ;
- la certification de conformité (aux exigences de l'annexe II du règlement) des dispositifs de création de signature et de cachet électroniques qualifiés ;
- la tenue du catalogue des dispositifs de création de signature / cachet électronique qualifiés qu'elle a certifié conformes.

IV. Questions relatives à la signature électronique

IV.1. Qu'est-ce qu'une signature électronique avancée ? Une signature électronique qualifiée ?

Une signature électronique avancée doit :

- être liée au signataire de manière univoque ;
- permettre d'identifier le signataire ;
- avoir été créé à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;
- être liée aux données qui lui sont associées de telle sorte que toute modification ultérieure des données soit détectable.

Une signature électronique qualifiée est une signature électronique avancée qui a été créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat qualifié de signature électronique.

L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

IV.2. Qu'est-ce qu'un dispositif de création de signature électronique qualifié ?

Un dispositif de création de signature électronique est un dispositif logiciel ou matériel configuré, servant à créer une signature électronique.

Un dispositif de création de signature électronique qualifié satisfait aux exigences de l'annexe II du règlement, et sert de support à la création des signatures électroniques qualifiées.

La conformité aux exigences de l'annexe II est certifiée par des organismes certificateurs désignés par chaque Etat membre à la Commission.

Pour les dispositifs de création de signature électronique qualifiés utilisés sous le contrôle exclusif du signataire, l'acte d'exécution n° 2016/650 référence les normes devant être utilisées pour prononcer la certification de conformité.

Pour les dispositifs de création de signature électronique qualifiés utilisés dans un environnement qui n'est pas sous le contrôle exclusif du signataire (i.e. dans le cas d'une « signature à distance »), il appartient à chaque Etat membre de définir le processus de certification de la conformité et de le notifier à la Commission.

IV.3. Quels sont les changements introduits par le règlement eIDAS pour la signature qualifiée ?

Le règlement eIDAS entraîne les changements suivants :

- Il permet explicitement la réalisation de signatures qualifiées « à distance » pour le compte du signataire, ces signatures devant être créées dans l'environnement d'un prestataire de services de confiance qualifié ;
- Il induit des obligations spécifiques pour les administrations (précisées ci-après) ;
- Il ne permet plus la délivrance de certificats de signature électronique pour les personnes morales (remplacés par les certificats de cachet électronique).

IV.4. Un face à face est-il nécessaire pour la délivrance d'un certificat qualifié de signature électronique ?

Le règlement prévoit que pour la délivrance d'un certificat qualifié pour un service de confiance, l'identité et tous les attributs de la personne physique ou morale à laquelle le certificat est délivré doivent être vérifiés. Il précise que cette vérification se fait :

- par la présence en personne de la personne physique ou du représentant autorisé de la personne morale (ce qui implique donc un face à face); ou
- à distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique (ou un représentant autorisé de la personne morale) s'est présenté en personne ; ou
- au moyen d'un certificat de signature électronique qualifié délivré conformément aux deux points ci-dessus ; ou
- à l'aide d'autres méthodes d'identification reconnues au niveau national et fournissant une garantie équivalente en termes de fiabilité à la présence en personne.

Un face à face peut ainsi ne pas être nécessaire, selon la méthode de vérification retenue parmi les possibilités offertes par le règlement.

IV.5. Pour le service de création d'une signature électronique avancée à distance, par quels moyens la personne peut-elle manifester son consentement ?

Dans le cas de la création d'une signature électronique avancée à distance, l'objectif est de s'assurer le niveau de sécurité assuré est similaire à celui d'une signature locale, où la réalisation de la signature électronique est réalisée sous le contrôle exclusif du signataire (*reposant par exemple sur une carte à puce et un code PIN*).

A cette fin, les moyens mis en œuvre doivent permettre de garantir un niveau de sécurité suffisant et de palier au risque de fraude à la signature. Pour ce faire, plusieurs solutions techniques peuvent être envisagées (*par exemple, la saisie d'un code PIN réservé à cet usage dans une application dédiée*), dans la mesure où l'implémentation faite de ces solutions est sécurisée.

IV.6. Quel est le régime de contrôle des prestataires de services de création de signature qualifiée à distance ?

Le règlement ne considère pas la création de signature qualifiée à distance comme un service de confiance qualifié.

Néanmoins, en vertu de l'annexe II du règlement, un prestataire de services de confiance mettant en œuvre un dispositif de création de signature électronique qualifié pour permettre la signature à distance pour le compte du signataire :

- doit avoir obtenu le statut qualifié de l'organe de contrôle, au titre de l'un des services de confiance qualifiés prévus par le règlement ;
- ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sans abaissement du niveau de sécurité et de manière proportionnée au besoin de continuité du service.

La vérification du respect de ces exigences est réalisée dans le cadre de la certification de conformité du dispositif de création de signature électronique qualifié.

IV.7. Quels sont les obligations faites aux administrations, pour l'usage de la signature électronique ?

Le règlement prévoit un mécanisme de reconnaissance mutuelle des signatures électroniques avancées, des signatures électroniques avancées reposant sur un certificat qualifié de signature électronique et des signatures électroniques qualifiées, utilisées dans le cadre de services en ligne offerts par un organisme du secteur public d'un Etat membre, et qui sont au moins dans les formats ou méthodes définies dans la décision d'exécution n° 2015/1506.

Les administrations exigeant une signature avancée doivent ainsi reconnaître les quatre formats de signature suivants:

- ETSI TS 103 171 (v.2.1.1) (XAdES Baseline Profile) ;
- ETSI TS 103 172 (v.2.2.2) (PAdES Baseline Profile) ;
- ETSI TS 103 173 (v.2.2.1) (CAdES Baseline Profile) ;
- ETSI TS 103 174 (v.2.2.1) (ASiC Baseline Profile).

De plus, le règlement prévoit que les organismes du secteur public ne peuvent pas exiger, pour une utilisation transfrontalière, de signature électronique présentant un niveau de sécurité supérieur à celui de la signature électronique qualifiée.

IV.8. Quel est l'impact du règlement eIDAS sur la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques ?

Le règlement eIDAS abroge la directive 1999/93/CE sur la signature électronique.

Le règlement prévoit des mesures de transition pour les produits et services qualifiés au titre de la transposition nationale de cette directive. Ces mesures sont détaillées ci-dessous.

IV.9. Quelles sont les modalités de transition entre la directive 1999/93/CE et le règlement eIDAS ?

Les modalités de transition entre la directive 1999/93/CE et le règlement eIDAS sont les suivantes :

- les dispositifs sécurisés de création de signature dont la conformité aux dispositions de la directive a été déterminée avant le 1er juillet 2016 seront considérés comme des dispositifs de création de signature qualifiés au sens du règlement eIDAS ;
- les certificats de signature électronique qualifiés délivrés aux personnes physiques au titre de la directive 1999/93/EC seront considérés comme des certificats qualifiés de signature électronique au titre du règlement eIDAS et ce jusqu'à leur expiration ;
- les prestataires de services de certification qui délivraient des certificats qualifiés au titre de la directive 1999/93/EC avant le 1er juillet 2016 seront qualifiés au sens du règlement eIDAS jusqu'au 1er juillet 2017. Au-delà de cette date, leur qualification ne sera maintenue que s'ils ont transmis un rapport d'évaluation de la conformité à l'organe de contrôle, et ce jusqu'à ce que ce dernier achève l'évaluation.

V. Questions relatives aux impacts nationaux du volet « services de confiance »

V.1. Que deviennent les lois, décrets et arrêtés pris en application de la directive 1999/93/CE suite à la parution du règlement eIDAS ?

Les dispositions des lois, décrets et arrêtés pris en application de la directive 1999/93/CE continuent à s'appliquer dans la mesure où elles ne sont pas en contradiction avec les dispositions du règlement eIDAS. Pour mémoire ces textes sont :

- Loi n° 2000-230 du 13 mars 2000 (prise en compte de la signature électronique dans le Code civil avec l'introduction de l'article 1316-4) ;
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique ;
- Arrêté du 26 juillet 2004 (relatif à la reconnaissance de la qualification des prestataires de service de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation).

V.2. Le RGS s'applique-t-il encore après la date d'application du règlement eIDAS ?

Le RGS continuera à s'appliquer pour partie suite à la parution du règlement eIDAS :

- d'une part, et en ce qui concerne ses destinataires, le règlement eIDAS s'applique aux échanges entre l'administration et le public (citoyens, entreprises) et ne s'applique pas aux « systèmes fermés » (c'est à dire sans impact direct sur les tiers);
- d'autre part, le périmètre fonctionnel du règlement eIDAS n'est pas identique à celui du RGS (ce dernier couvre notamment la délivrance de certificats d'authentification de personnes ou de machines, et la délivrance de certificats de confidentialité, qui sont deux services non couverts par le règlement) ;
- enfin, le règlement n'induit pas d'obligation pour les administrations de recourir à des moyens d'identification électronique notifiés ou à des services de confiance qualifiés au titre du règlement eIDAS.

V.3. Les produits certifiés conformes (carte à puce, HSM) au décret 2001-272 sont-ils qualifiés au titre du règlement eIDAS ?

Les mesures de transition prévues pour la directive 1999/93/CE s'appliqueront à ces produits. Ainsi, conformément à ces mesures de transition, les dispositifs sécurisés de création de signature électronique conformes aux dispositions de la directive seront considérés comme des dispositifs de création de signature électronique qualifiés au sens du règlement eIDAS.

V.4. Quel impact a le règlement eIDAS sur le décret 2011-434 relatif à l'horodatage électronique ?

En raison du principe de continuité du droit, la plupart des dispositions du décret n°2011-434 étant compatibles avec le règlement eIDAS, le décret ne sera pas abrogé. Toutefois, les dispositions incompatibles et notamment l'article 6 ne seront plus applicables et seront automatiquement remplacées par les dispositions du règlement les plus adéquates.

V.5. Les services qualifiés au titre de l'arrêté du 26 juillet 2004 ou du RGS sont-ils qualifiés au titre du règlement eIDAS ?

Les prestataires de services de confiance qualifiés selon l'arrêté du 26 juillet 2004 ou selon le RGS (prestataires de services de certification électronique qualifiés au niveau 2 étoiles ou 3 étoiles, prestataires de services d'horodatage électronique) bénéficieront de modalités de qualification facilitées au titre du règlement eIDAS.

Les autres services prévus par le règlement (création de signature à distance, validation de signature, conservation de signature, envoi recommandé électronique) n'étaient pas couverts par la règlementation française et il n'existe donc pas de facilité de qualification particulière les concernant.

V.6. Quel impact a le règlement sur les professions réglementées et sur les textes qui les encadrent ?

Le décret n°2005-972 (pour les huissiers) et le décret n°2005-973 (pour les notaires) renvoient au décret n°2001-272 pour l'utilisation de la signature électronique qualifiée. Par conséquent les mesures de transition prévues par le règlement s'appliqueront.