Commerce électronique
La confiance électronique, entre droit et technique

Les apports du règlement européen sur l'identification électronique et les services de confiance

Le règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)[1] est entré en vigueur le 17 septembre 2014 et devrait être applicable - pour certaines dispositions - le 1er juillet 2016[2].
Ce règlement touche à des domaines aussi variés que l'identification électronique étatique, les signatures, les cachets, l'horodatage, les certificats d'authentification de site, les documents ou les services d'envois recommandés électroniques, éléments constitutifs de la confiance électronique sur le marché intérieur... Concomitamment, il définit les conditions de cette confiance en s'appuyant sur le régime des Prestataires de Services de Confiance (PSCo) et les modalités de leur contrôle.

LES RAISONS DU RÈGLEMENT EIDAS

La directive 1999/93/CE relative à la signature électronique[3] a introduit la signature électronique afin d'assurer la sécurité et la confiance sur les réseaux numériques dans l'Union européenne. Toutefois, ces instruments n'ont jamais connu l'essor attendu ou espéré comme le constate le résumé de l'analyse d'impact accompagnant la proposition de règlement[4]. L'harmonisation réalisée par la transposition de la directive 1999/93/CE dans les droits nationaux n'a donc pas atteint les objectifs et les usages de la signature ne se sont encore actuellement que peu développés.

En outre, confronté au déploiement du commerce électronique, le marché de la confiance électronique s'est étoffé, les technologies multipliées : l'horodatage, les envois recommandés électroniques mais aussi certains usages du certificat (qui n'existaient pas encore) se sont déployés...

Dès lors, la Commission a choisi la voie du règlement européen, instrument juridique directement applicable dans tous les Etats membres sans interprétation ni adaptation[5], par souci de rapidité (« time to law ») et de simplicité (remplacement pur et simple des dispositions nationales existantes en la matière) en prévoyant un régime juridique propre à l'identification électronique étatique, en étendant le périmètre des services de confiance au-delà des seuls certificats électroniques et en établissant un cadre juridique aux PSCo.

L'IDENTIFICATION ÉLECTRONIQUE, NOUVEAU SÉSAME ÉTATIQUE ?

Le chapitre II du règlement eIDAS est spécifique à l'identification électronique étatique[6], c'est-à-dire celle « exigée en vertu du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre » (art. 6.1) ; il s'agit donc de déterminer les conditions de gestion et de délivrance de moyens d'identification électronique en se fondant sur un schéma d'identification électronique notifié (art. 7). De plus, les moyens d'identification ainsi notifiés pourront disposer d'un niveau de garantie (art. 8 et 9) : faible, substantiel ou élevé. Les conditions formelles entourant cette notification[7] ainsi que les mesures de sécurité propres à chaque niveau de garantie[8] figurent dans des actes d'exécution en cours de rédaction par le CEN (Comité européen de normalisation) et l'ETSI (l'European Telecom Standards Institute).

Le règlement se concentre avant tout sur les approches transfrontalières[9] de reconnaissance et d'acceptation mutuelle de l'identification électronique étatique. Les Etats devront toutefois être particulièrement vigilants quant à la sécurité du système d'identification notifié (art.10), toute atteinte à la sécurité ou toute mauvaise attribution du moyen d'identification à son titulaire légitime pouvant engager sa responsabilité envers toute personne morale ou physique (art.11). Les questions relatives à l'engagement de l'Etat sur ce fondement sont nombreuses et nécessiteront des développements ultérieurs.

On notera que l'Etat français est en train de déployer un outil de fédération d'identités commune à tous les services en ligne des administrations : France Connect. Cet outil permettra à chaque usager inscrit – sans que cette inscription soit obligatoire – de ne pas avoir à effectuer une telle démarche spécifiquement sur chaque site administratif : il lui faudra juste

se connecter avec son profil unique à tous les services administratifs[10]. La démarche de validation du projet est en cours auprès de la Cnil mais rien n'est encore indiqué concernant sa conformité avec le règlement eIDAS.

LES SERVICES DE CONFIANCE VISÉS

Les services de confiance visés dépassent désormais la signature électronique et prennent en compte d'autres outils de la confiance numérique.

Quid de la signature électronique ?

La directive 1999/93/CE est en passe d'être abrogée (art. 50), les nouvelles dispositions relatives à la signature électronique qui seront applicables le 1er juillet 2016 prennent en compte ses différents aspects. Le règlement eIDAS énonce ainsi que « l'effet juridique d'une signature électronique qualifiée est équivalente à celui d'une signature manuscrite » (art. 25.2), ce qui n'est pas expressément prévu dans le code civil français. Cela ne signifie pas pour autant que le recours à une signature électronique qualifiée dispenserait le signataire de rapporter la preuve lors d'une vérification d'écriture : elle serait - comme les signatures manuscrites - soumise aux articles 287 et s du code de procédure civile[11] .

Allant au-delà des dispositions existantes, le règlement eIDAS prévoit également : les conditions entourant la vérification (art. 33) et la conservation des signatures électroniques qualifiées (art. 34), ce qui constitue une première prise en considération de l'archivage des données associées à l'échelle européenne[12];
ainsi que des dispositions particulières relatives à la signature électronique dans les services publics (art. 26). Ainsi, les Etats membres ne peuvent exiger une signature plus sécurisée que la signature électronique qualifiée de la part de citoyens de l'Union européenne et en créant une hiérarchie des signatures pour ce secteur.
De plus, le considérant 52 du règlement intègre également la signature électronique centralisée (« remote electronic signature »), c'est-à-dire activée à distance[13] comme les signatures électroniques « à la volée », ce qui constituera une réelle avancée pour le marché dans l'attente d'une reconnaissance de ce type de signature.

Quels autres services de confiance ?

Fondés sur le même principe technique que la signature électronique, le règlement eIDAS a introduit les cachets électroniques (art. 34), « sceaux » propres à une personne morale garantissant l'origine et l'intégrité des données associées (sans manifestation du consentement contrairement à la signature). Ce sont des signatures « techniques » vérifiées à l'aide d'un certificat serveur[14]. Ils seront utilisés pour valider juridiquement une multitude de documents, échanges ou transactions électroniques au même titre qu'une griffe[15] au sens commercial du terme.

Dans le même ordre d'idée, les certificats d'authentification de sites web (art. 43) sont destinés à la sécurisation des échanges, utilisés par les sites marchands, et permettent de sécuriser la connexion ainsi établie entre un client et un serveur. Il s'agit d'un moyen efficace pour lutter contre le phishing ; l'utilisateur peut vérifier que le site sur lequel il se trouve est bien celui qui s'est authentifié. Cette question est d'ailleurs détaillée dans les recommandations de sécurité de l'Anssi concernant l'analyse des flux https[16].

Les services de confiance ont également trait à la datation des échanges, autre élément essentiel des transactions électroniques[17] que ce soit :
- pour des services d'horodatage électronique (art. 39), déjà prévus en droit français[18] , permettant de garantir l'exactitude de la date et de l'heure indiquées et de l'intégrité des données auxquelles se rapportent cette date et cette heure ;
- ou pour des services d'envois recommandés électroniques (art. 41), là encore insérés en droit français (art. 1369-8 du code civil et décret n° 2011-144 du 2 février 2011 relatif à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat[19]), bénéficiant d'une « présomption quant à l'intégrité des données, à l'envoi par l'expéditeur identifié et à la réception par le destinataire identifié des données et à l'exactitude de la date et de l'heure indiquées par le service d'envoi recommandé électronique qualifié concernant l'envoi et la réception ». On notera qu'en droit administratif, une ordonnance n° 2014-1330 du 6 novembre 2014 relative au droit des usagers de saisir l'administration par voie électronique[20] vient préciser les conditions d'envois ou de réceptions « recommandés » par voie électronique entre un usager et une autorité administrative[21].

Enfin, le règlement eIDAS prévoit les conditions de non-discrimination[22] médiatique des documents électroniques vis-à-vis des documents papier (art. 44), dont l'efficacité juridique et la recevabilité comme preuves en justice ne peuvent être déniées au motif de leur forme électronique.

Il est essentiel de rappeler que le règlement eIDAS est d'application volontaire pour les acteurs du marché, désireux de disposer ou de distribuer de produits ou services de confiance à l'échelle européenne[23]. Les services de confiance qualifiés constituent donc un précieux sésame quant à leur interopérabilité et leur acceptation au sein du marché intérieur. Dès lors, on peut estimer que la démarche - volontaire - de certains PSCo constituera une des conditions de la confiance ; la fiabilité de leurs pratiques ou de leurs produits étant reconnue dans chaque Etat membre de l'UE.

LE RÉGIME JURIDIQUE DES PSCO

Le prestataire de services de confiance (PSCo) se définit au sens de l'art. 3.19 comme « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié », c'est-à-dire en charge de la gestion des services de confiance ci-avant évoqués. Rien n'indique que ce prestataire doit être

un tiers à une transaction électronique. Ainsi, même si, souvent, les juristes évoquent le principe figurant sous l'article 1315 du code civil selon lequel « Nul ne peut se constituer de preuve à lui-même », il reste envisageable que des PSCo inclus par exemple dans un groupe de sociétés (par exemple, une autorité de certification propre à un groupe bancaire ou de télécommunications) dont les pratiques sont auditables, traçables et fiables puissent établir des signatures électroniques ou d'autres services de confiance sans être pour autant tiers.

La responsabilité des PSCo est essentielle dans le dispositif mis en place à l'échelle européenne. L'article 13-1 rappelle les principes de responsabilité de droit commun puisque ce sera à celui qui invoque des dommages par le PSCo non qualifié de rapporter la preuve de l'intentionnalité ou de la négligence. A contrario, conformément à l'art.13-1, le PSCo qualifié sera présumé responsable, charge pour ce dernier de rapporter la preuve inverse. De plus, le PSCo devra informer ses utilisateurs des limites relatives à l'utilisation des services. Ces règles s'appliquent conformément aux règles nationales en matière de responsabilité (art. 13-3).

Les PSCo, qualifiés ou non, devront, conformément à l'article 19, prendre les « mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque ». Cette obligation de sécurité (qui pourrait varier d'obligation de moyens renforcés pour les PSCo non qualifiés à obligation de résultat pour les PSCo qualifiés) est couplée avec une obligation de notification des atteintes à la sécurité des données ou de toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel conservées (art. 19-2) dans un délai de 24 heures après en avoir eu connaissance auprès des organismes nationaux en charge de la sécurité informatique (Agence nationale de la sécurité des systèmes d'information, Anssi en France) et de l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information). Le formalisme se rapproche de celui relatif aux failles de sécurité au sens de la norme ISO 27001[24].

Lorsqu'il est qualifié, le PSCo est, de plus, responsable du non-respect des exigences directement applicables (art. 19) et qui renvoient ici à des mesures organisationnelles qu'il doit mettre en œuvre. Pour tous les PSCo qualifiés fournissant des services de confiance (art. 24-2), des mesures organisationnelles globales (personnel compétent, responsabilité des dommages causés, informations précontractuelles, fiabilité des produits et systèmes, mesures contre les fraudes et falsifications…) seront à mettre en œuvre. Eu égard à l'importance prise par les certificats dans le cadre du marché européen de la confiance, des dispositions particulières lui seront applicables[25].

QUEL CONTRÔLE POUR LES PSCO ?

Le contrôle des PSCo qualifiés se décline autour d'un audit annuel effectué par l'organisme national désigné à cet effet (l'Anssi en France selon toute vraisemblance) pour vérifier que ces derniers respectent les obligations énoncées dans le règlement (art. 20.1 et s.) et d'un pouvoir contraignant a priori ou a posteriori des organes de contrôle en vue de corriger tout manquement constaté aux obligations du règlement (art. 20.3). A défaut de correction dans un délai fixé, le PSCo perdra son statut qualifié (art. 20.3) ; ce qui aura une incidence sur les listes de confiance publiées par les Etats membres.

Les PSCo non qualifiés sont, eux aussi, soumis à un contrôle a posteriori lorsque les organismes de contrôle soupçonnent qu'ils ne respectent pas les exigences posées dans le règlement (art. 17.3-b).

La disponibilité de l'information relative à la qualification d'un service de confiance ou d'un PSCo constitue un critère essentiel du choix de tel ou tel PSCo. C'est pourquoi chaque Etat membre doit établir, tenir à jour et publier des listes de confiance à ce sujet (art. 22). Elles doivent être établies, mises à jour et tenues de façon sécurisée, dans les meilleurs délais (art. 22.3) et être facilement accessibles.

Enfin, un label de confiance[26] (art. 23) permettra de distinguer les services de confiance qualifiés des autres.

Comme en témoignent les multiples actes d'exécution que les acteurs du marché attendent, le droit de la confiance numérique est largement influencé par la technique. D'ailleurs, la majorité de ces actes permettra si nécessaire, de désigner des normes dont le respect entrainera une présomption de conformité aux exigences du règlement. D'autres actes consisteront à définir des procédures applicables aux autorités publiques.

Les actes obligatoires du règlement serviront à définir un cadre d'interopérabilité des moyens d'identification, un label de confiance pour les prestataires de services qualifiés, le format de la «liste de confiance» ou les formats de signature pour les signatures électroniques « publiques ». En ce sens, la Commission européenne s'appuiera sur des normes techniques (European Norm – EN) obligatoirement applicables (au détriment d'autres normes nationales qui seraient contraires aux normes européennes).

Toutefois, aucune automaticité technique ne pourra permettre à un service de confiance de produire ses effets sans qu'un juge puisse y trouver à redire car c'est bien là le défi de ce règlement : faire cohabiter intelligemment européen et national, technique et droit, sans que cette cohabitation tourne à une situation kafkaïenne.

Pascal AGOSTI
Avocat associé
Cabinet Caprioli
Docteur en droit

Notes

(1) JOUE L. 257 du 28 août 2014, p. 73 et s. Pour plus de détails, voir E. Caprioli, Signature électronique et dématérialisation, éd. LexisNexis, 2014 ; concernant la proposition de règlement, E. Caprioli, P. Agosti, la régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, Comm. Com. Electr., n° 2, février 2013, p. 10-19 ; Th. Piette-Coudol, Une législation européenne pour la signature électronique (À propos du règlement européen sur l'identification électronique et les services de confiance), Droit de l'immatériel, n° 84, juillet 2012, p. 78-87.

(2) Notons toutefois que la période de transition entre la directive 1999/93/CE et le règlement eIDAS devrait se terminer au 1er juillet 2020, date d'expiration du dernier certificat qualifié au sens de la directive 1999/93/CE. V. pour les autres dates d'entrée en vigueur, l'article 52 du règlement eIDAS.

(3) Directive 1999/93/CE du 13 décembre 1999 (directive 1999/93/CE du 13 décembre 1999, JOCE n° L. 13, 19 janvier 2000, p.12 s ; E. Caprioli, La directive européenne n°1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Gaz. Pal. du 29 octobre au 31 octobre 2000, p. 5 et s).

(4) Le résumé de l'analyse d'impact (COM (2012) 238 final), p. 3, énonce différentes causes cumulatives :

- la fragmentation du marché : les prestataires de services sont soumis à des règles différentes en fonction des États membres qu'ils desservent.
- le manque de confiance : le manque de confiance dans les systèmes électroniques, dans les outils fournis et dans le cadre juridique peut donner l'impression que les garanties juridiques sont moindres que dans le cas d'une interaction physique en raison :
  d'un cadre juridique actuel insuffisamment développé ;
  - d'un manque de coordination dans le développement des signatures et de l'identification électroniques ;
  - du manque de transparence des garanties de sécurité ;
  - du manque de sensibilisation/d'adhésion des utilisateurs.

(5) « L'adoption d'une directive ne permettrait pas de résoudre les problèmes actuels d'interopérabilité dans le domaine des signatures électroniques, dus à des divergences dans la transposition de la directive 1999/93/CE. En revanche, un règlement, qui est directement applicable sans interprétation, garantit une meilleure harmonisation et est par conséquent approprié pour atteindre les objectifs de la législation proposée. », Résumé de l'analyse d'impact, p.8.

(6) V. Th. Piette-Coudol, L'identification électronique peut-elle se fonder sur les papiers d'identité ?, RLDI Octobre 2014, p.71 et s. Ainsi les dispositions relatives à l'identification réalisée par une entreprise (Facebook Connect par exemple) ne sont pas applicables.

(7) Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the inter-nal market, Phase II - eID notification, Version 2.1, 5 juin 2014, §3.1 : « As described above, the Implementing act should define "the circumstances, formats and procedures of the notification". This logical structure can be applied to the Implementing Act, which should thus consist of three substantive sections:

- Circumstances for notification ;
- Content and format of the notification ;
- Procedures for the notification. ».

(8) Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market, Phase II - eID security assurance levels, Version 2.1, 5 juin 2014.

(9) Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market, Phase II - Cross border interoperability cooperation group, Version 2.1, 5 juin 2014.

(10) V. notamment France Connect : la fédération d'identité des citoyens pour toutes les administrations, Bertrand Lemaire, 7 octobre 2014, http://www.cio-online.com/actualites/lire-france-connect%C2%A0-la-federation-d-identite-des-citoyens-pour-toutes-les-administrations-7119.html.

(11) J. Devèze, Perserverare diabolicum. A propos de l'adaptation du droit de la preuve aux technologies de l'information par le décret n° 2002-1436 du 3 décembre 2002, Comm. Com. Electr. 2003, chr. 8.

(12) Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market, Phase II - Reference numbers of standards for the qualified preservation service for qualified electronic signatures, Version 2.1, 5 juin 2014, § 2.2 : « The preservation of the signed data also matters and can hardly be dissociated from the preservation of a QES [Qualified Electronic Signature]».

(13) « La création de signatures électroniques à distance, système dans lequel l'environnement de création de signatures électroniques est géré par un prestataire de services de confiance au nom du signataire, est appelée à se développer en raison de ses multiples avantages économiques. Toutefois, afin que ces signatures électroniques reçoivent la même reconnaissance juridique que les signatures électroniques créées avec un environnement entièrement géré par l'utilisateur, les prestataires offrant des services de signature électronique à distance devraient appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire. [...] » ; V. F. Leroy, Trustworthy Systems Supporting Server Signing, Document de travail CEN, Inédit.

(14) Comme pour les factures électroniques en France qui sont « signées » avec une vérification liée à un certificat serveur ; voir E. Caprioli, Les nouvelles règles fiscales applicables en matière de facturation électronique, Comm. Com. Electr., n° 3, mars 2013, com. 36 ; Th. Piette-Coudol, Un chantier de dématérialisation exemplaire : la facture électronique au 1er janvier 2013, RLDI n° 92, avril 2013, p. 62-77.

(15) Ch. Gavalda, La validité de certaines signatures à la griffe d'effets de commerce, JCP éd. G, 1966, I, 2034.

(16) Recours au protocole TSL, disponible à l'adresse http://www.ssi.gouv.fr/IMG/pdf/NP_TLS_NoteTech.pdf.

(17) L. Jacques, La date électronique et le contrat, in Les deuxièmes journées internationales du droit du commerce électronique, Actes du colloque organisé par l'EDHEC et l'Ecole du droit de l'entreprise de l'Université de Montpellier, Nice 6 et 7 novembre 2003, Paris, Ed. Litec, n° 22, Collection Actualités du droit de l'entreprise, mars 2005, p.165 et s.

(18) Décret n°2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, JO du 21 avril 2011, p.7093 ; v. égal. l'arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

(19) JO du 4 février 2011 p.2274 ; v. E. Caprioli, La lettre recommandée électronique, un nouveau décret pour la « confiance numérique » ; Comm. Com. Electr., n° 4, avril 2011, com. 40. ; L. Grynbaum, Pour une bonne réception de la lettre recommandée électronique, JCP G, n° 7, 28 février 2011, 162.

(20) JO du 7 novembre 2014 p. 18780.

(21) « Art. 5-2. - I. - Lorsqu'il est requis que l'envoi d'un document par un usager à une autorité administrative se fasse par lettre recommandée, cette formalité peut être satisfaite par l'utilisation d'un téléservice ou d'un procédé électronique, accepté par ladite autorité administrative, permettant de désigner l'expéditeur et d'établir si le document a été remis ou non à cette autorité.

« II. - Lorsqu'il est requis qu'un document administratif soit notifié à l'usager par lettre recommandée et après avoir recueilli l'accord exprès de l'usager, cette formalité peut être satisfaite par l'utilisation d'un procédé électronique permettant de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si le document a été remis ou non au destinataire.

« Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat. ».

(22) Le principe de non discrimination à l'égard des engagements sous forme électroniques est apparu pour la première fois à l'article 5 de la loi-type de la CNUDCI sur le commerce électronique, et ensuite dans les directives européennes n°1999/93/CE et n°2000/31/CE. V. en ce sens : Eric A. Caprioli, Arbitrage international et commerce électronique, RLDI 2012, Avril, v. p.116.

(23) L'art. 2.2. du Règlement eIDAS dispose : « Le présent règlement ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants ».

(24) V. en ce sens, Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market, Phase II - Common provisions on TSPs s, Version 2.1, 4 juin 2014, § 3.1.1 concernant les Due Diligence des PSCo : « ISO/IEC 27001: ISO 27000 series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS). Not about IT only as it covers all aspects of information exchange, from computer data to conversations in public areas, including securing of physical perimeters and initial person-nel screenings. It helps to assure business continuity under almost all circumstances. It is possible for an organization to put in place a policy on information security that covers all forms of commu-nication and data storage. ISO 27001 is the backbone of this. Assessment (e.g. self, 3rd party, certification) against ISO/IEC 27001 ISMS requirements1 is possible today for large, medium and small enterprises in every sector.». V. égal. Sur les notifications : Loi n° 2013-1168, 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale : JO 19 décembre 2013, p. 20570; E. Caprioli, La loi de programmation militaire et sécurité de l'information, CCE Mai 2014, Comm. N°50. Le nouvel article L. 1332-6-2 du Code de la défense prévoit une procédure de notification au profit des Opérateurs d'Importance Vitale.

(25) Par exemple, l'article 24-1 prévoit que le PSCo devra vérifier « par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié ». La vérification peut être effectuée en face à face avec la personne physique ou le mandataire de la personne morale ou à distance à l'aide d'un système notifié d'identification (art. 24.1-b). De plus, ils doivent enregistrer et publier la révocation d'un certificat dans leur base de données dans un délai de 24 heures à compter de la demande (art. 24.3) et mettre à disposition de toute partie utilisatrice des informations sur la validité ou la révocation des certificats qualifiés qu'ils ont délivrés, disponibles à tout moment de façon automatique, fiable et gratuite (art. 24.4). La Commission dispose du pouvoir de déterminer, par des actes d'exécution, les numéros de référence des normes applicables aux systèmes et produits fiables (art. 24.5).

(26) Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market, Phase II - Supervision EU trust mark for qualified trust services, Version 2.1, 4 juin 2014.