universign

powered by Cryptolog

LIVRE BLANC

QUE RETENIR DU NOUVEAU RÈGLEMENT EUROPÉEN SUR LA SIGNATURE ÉLECTRONIQUE ?

13 points pour décrypter le règlement eIDAS

www.universign.com

TABLE DES MATIÈRES

INTRODUCTION

Le 23 juillet 2014, le Conseil de l'Union Européenne annonçait l'adoption définitive du nouveau règlement dit eIDAS (Electronic Identification And trust Services), sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Publié le 28 août au journal officiel de l'Union Européenne sous la référence (UE) n°910/2014, ce texte engendre un profond renouvellement du cadre juridique européen sur les services de preuve électronique. Il faut dire que celui-ci n'avait pas connu de modification depuis la directive de 1999 sur la signature électronique. Or, ce règlement n'est pas une simple actualisation de la directive : il vient l'abroger et offre la promesse de voir émerger un véritable marché paneuropéen de la confiance numérique, là où précisément l'application d'une directive s'est révélée être un échec. Et ce, au grand bénéfice des utilisateurs qui pourront bénéficier d'un espace unique et sécurisé pour la plupart des transactions électroniques en Europe.

Paradoxalement, ce nouveau règlement est passé relativement inaperçu dans les média, sans doute en raison de sa complexité d'approche. En effet, comme toujours en matière de confiance numérique, le texte est technique, jargonneux et difficilement comestible pour les non-initiés. En tant qu'experts du sujet, nous nous sommes sentis obligés d'en révéler l'importance en vous livrant dans un document ses principales clés de compréhension.

Aujourd'hui, cela ne fait plus aucun doute : entre une demande du marché chaque jour toujours plus forte et un nouveau cadre règlementaire européen tirant parti des erreurs du passé, nous sommes bien à l'aube d'une nouvelle ère pour la signature électronique.

Bonne lecture !

1 L'APPLICATION D'UN RÈGLEMENT ET PAS D'UNE DIRECTIVE

Notre analyse

La directive 1999/93/CE couvrait essentiellement les signatures électroniques sans fournir de cadre transnational et intersectoriel complet pour des transactions électroniques sûres, fiables et aisées.

Elle définissait une sorte de « schéma directeur » que chaque nation européenne devait transposer dans sa législation nationale. Cela a abouti à une reconnaissance de la signature électronique dans l'ensemble des pays européens, mais à une application législative différente : chaque pays a défini sa propre loi, rendant ainsi les échanges européens plus complexes.

À la différence de la directive, ce nouveau règlement communautaire s'appliquera totalement et directement en Europe et ne donne pas de possibilité de transpositions législatives nationales par les États. Il vient abroger la 1999/93/CE à partir du 1er juillet 2016 et s'appliquera en effet directement à partir de cette date dans tous les états membres de l'UE. Il viendra remplacer les lois nationales, ce qui engendrera des modifications profondes dans la législation de certains pays en matière de signature et d'identification électronique. De même, les référentiels nationaux, comme le RGS, devront se mettre en conformité avec ce règlement.

Extraits du règlement

« **Article 50**

Abrogation

1. La directive 1999/93/CE est abrogée avec effet au 1er juillet 2016. »

« **Article 52**

Entrée en vigueur

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

2. Le présent règlement est applicable à partir du 1er juillet 2016 [...] »

2 UN CHAMP D'APPLICATION PLUS VASTE QUE LA DIRECTIVE DE 1999

Notre analyse

Alors que la directive ne s'intéressait qu'à la signature électronique, le règlement instaure un cadre juridique beaucoup plus général pour différents types de transactions électroniques au sein du marché intérieur.

À l'instar de ce qui avait été fait en France avec le RGS, le règlement définit et encadre l'utilisation de différents types de services de confiance qui vont de l'identification électronique à l'authentification de sites Internet (certificats SSL) en passant par l'horodatage, la signature, le cachet électronique, et les services d'envois recommandés électroniques.

Extraits du règlement

« **Article premier**

Objet

En vue d'assurer le bon fonctionnement du marché intérieur tout en visant à atteindre un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance, le présent règlement :

a) fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre,

b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques, et

c) instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envoi recommandé électronique et les services de certificats pour l'authentification de sites internet. »

3 UN DOCUMENT ÉLECTRONIQUE EST UNE PREUVE

Notre analyse

C'est la première fois qu'un texte fait aussi explicitement référence à la notion de « document électronique » tout en lui conférant une valeur probatoire.

Le chapitre IV du règlement stipule en effet qu'un document électronique ne peut pas être refusé au titre de preuve en justice au seul motif qu'il se présente sous forme électronique. Dans un monde où le numérique fait encore trop souvent peur, cela a le mérite d'être écrit dans la loi !

Extraits du règlement

« **Article 46**

Effets juridiques des documents électroniques

L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique. »

4 DES SERVICES DE SÉCURITÉ LABELLISÉS DANS TOUTE L'EUROPE

Extraits du règlement

« **Article 20**

Contrôle des prestataires de services de confiance qualifiés

1. Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'organe de contrôle dans un délai de trois jours ouvrables qui suivent sa réception. »

Notre analyse

Pour chaque type de service (identification, signature, horodatage, etc.), le règlement définit la notion de service de confiance qualifié et de prestataire de service de confiance qualifié. Ces opérateurs auront un certain nombre d'exigences de sécurité à respecter et devront subir un processus de certification afin de vérifier qu'ils sont conformes au règlement.

En contrepartie, les utilisateurs de ces services jouiront le cas échéant d'un effet juridique fort et bénéficieront d'une présomption de fiabilité quant aux preuves électroniques apportées en cas de contentieux. À titre d'exemple, « les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et 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 par le service d'envoi recommandé électronique qualifié ».

Pour identifier les services qualifiés, un label de confiance sera créé et utilisé sur les sites web des prestataires de services de confiance qualifiés dans l'ensemble des 28 pays de l'Union Européenne. Un tel label distinguera clairement les services de confiance qualifiés d'autres services de confiance, contribuant ainsi à la transparence du marché. Fini les Tiers de confiance autoproclamés, les accréditations imaginaires, les argumentaires de preuves bancals et complexes. Les internautes seront donc immédiatement informés qu'ils peuvent faire confiance à un service en ligne lorsqu'ils effectuent une transaction électronique. Ils seront assurés d'utiliser un service audité qui applique scrupuleusement les normes et règles européennes en termes de sécurité, de qualité, de respect de la réglementation, de continuité de services, de protection de la vie privée...

5 LA CONSÉCRATION DES LISTES DE CONFIANCE

Notre analyse

Imposées depuis plusieurs années par la Commission Européenne aux États membres, les listes de confiances sont des services en ligne qui ont pour but de regrouper les listes de fournisseurs de services de confiance, considérés comme des références fiables par les différents États de l'Union.

Bien évidemment, le règlement ne manque pas de faire référence à ces outils puisque les différents États seront désormais tenus de référencer dans ces listes, les services et les prestataires qualifiés et labellisés au sens du règlement européen.

Accessible par des machines ou par des utilisateurs, ces listes constitueront un référentiel indiscutable pour vérifier qu'une signature, un cachet serveur, un horordatage est qualifié, et qu'un service respecte cette nouvelle règlementation européenne.

Extraits du règlement

« **Article 22**

Listes de confiance

"1. Chaque État membre établit, tient à jour et publie des listes de confiance, y compris des informations relatives aux prestataires de services de confiance qualifiés dont il est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent.

2. Les États membres établissent, tiennent à jour et publient, de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance visées au paragraphe 1 portant une signature électronique ou un cachet électronique.

3. Les États membres communiquent à la Commission, dans les meilleurs délais, des informations relatives à l'organisme chargé d'établir, de tenir à jour et de publier les listes nationales de confiance, ainsi que des détails précisant où ces listes sont publiées, indiquant les certificats utilisés pour apposer une signature électronique ou un cachet électronique sur ces listes et signalant les modifications apportées à ces listes.

4. La Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées au paragraphe 3 sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé. »

6 UNE HARMONISATION PANEUROPÉENNE DE LA SIGNATURE ÉLECTRONIQUE

Extraits du règlement

« **Article 25**

Effets juridiques des signatures électroniques

1. L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

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

3. Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres. »

Notre analyse

C'est l'une des grandes forces de ce règlement dans la mesure où la directive a montré ses limites en termes d'harmonisation européenne de la signature électronique. Celle-ci ayant été transposée de manière différente dans chacun des États membres, il existe aujourd'hui autant de manières de « faire de la signature électronique » en Europe qu'il y a d'États dans l'Union Européenne !

Le règlement - et les actes d'exécution délégués qui vont suivre - vont mettre tout le monde d'accord en ne donnant pas aux états la possibilité d'intervenir sur la manière d'implémenter une signature électronique et en particulier une signature électronique qualifiée. Le règlement définit en effet la signature électronique qualifiée comme une signature équivalente en justice à la signature manuscrite.

En d'autres termes, une signature qualifiée pourra bénéficier de présomption de fiabilité devant tous les tribunaux européens. Non seulement, un juge polonais ne pourra plus refuser une signature électronique faite par un espagnol avec une solution française, mais de surcroît il devra la considérer d'emblée comme fiable si elle dispose du label de signature qualifiée.

Ce règlement crée donc les conditions d'un véritable marché européen de la confiance numérique dans lequel vont pouvoir se développer les acteurs du secteur sans avoir à souffrir de protectionnismes nationaux.

7 LA FIN DU DOGME DE LA CARTE À PUCE

Notre analyse

La directive de 1999 préconisait l'usage de certificats sur supports physiques sécurisés pour obtenir un niveau maximal force probante aux documents signé électroniquement. Le règlement introduit un assouplissement des règles juridiques à respecter pour bénéficier de la présomption de fiabilité auprès de tous les tribunaux Européens : le recours à un support physique qualifié ne fait pas partie des exigences applicables aux dispositifs de création de signature électronique qualifiés, permettant d'obtenir un niveau de sécurité juridique maximal sur les documents signés. Le règlement envisage d'ailleurs explicitement que les clés privées de signature – appelées données de création de signature électronique en jargon juridique – soient confiées à des prestataires de services de confiance qualifié.

Ce nouveau cadre juridique ouvre donc la voie aux solutions de signature à distance (Cloud) et de signature sur mobiles ou tablettes.

Extraits du règlement

« (51) Le signataire devrait pouvoir confier les dispositifs de création de signature électronique qualifiés aux soins d'un tiers pour autant que des mécanismes et procédures appropriés soient mis en œuvre pour garantir que le signataire a le contrôle exclusif de l'utilisation de ses données de création de signatures électroniques, et que l'utilisation du dispositif satisfait aux exigences en matière de signature électronique qualifiée.

(52) 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 [...] »

« ANNEXE II
EXIGENCES APPLICABLES AUX DISPOSITIFS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE QUALIFIÉS

3. La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié. »

8 LE MAINTIEN DU FACE-À-FACE

Notre analyse

Avec la directive Européenne de 1999, le RGS, ou même l'arrêté du 26 juillet 2004, la délivrance d'un certificat qualifié imposait une vérification d'identité en face à face par une autorité de certification qualifiée.

Autrement dit, jusqu'à présent un face-à-face était requis pour obtenir un niveau maximal force probante aux documents signé électroniquement.

Le règlement ne déroge pas à la règle puisqu'il impose toujours aux prestataires de services qualifiés de vérifier l'identité du demandeur en sa présence lors de la remise d'un certificat qualifié.

Extraits du règlement

« **Article 24**

Exigences applicables aux prestataires de services de confiance qualifiés

1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, 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.
Les informations visées au premier alinéa sont vérifiées par le prestataire de services de confiance qualifié directement ou en en ayant recours à un tiers conformément au droit national :

a) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale […] »

9 UNE RECONNAISSANCE MUTUELLE DES IDENTIFICATIONS ÉLECTRONIQUES ~~EN EUROPE~~

Notre analyse

Le règlement accorde une place très importante aux dispositifs d'identification électronique ~~qui sont traités dans ce texte de manière indépendante des autres services de confiance.~~ Il définit trois niveaux d'identification qui diffèrent en fonction de leur degré de fiabilité : niveau de garantie faible, substantiel et élevé.

La manière d'implémenter ces différents niveaux sera documentée dans les actes d'exécution et les normes à venir.

Le règlement encourage l'implémentation des niveaux substantiel et élevé. L'idée est d'aboutir à une interopérabilité des moyens d'identification électronique en Europe : en résumé, tous les services publics européens devront pouvoir accepter les moyens d'identifications substantiel et élevé, quels que soient les États qui les ont mis en service.

Extraits du règlement

« **Article 6**

Reconnaissance mutuelle

1. Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est 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, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne, à condition que les conditions suivantes soient remplies :

a) ce moyen d'identification électronique est délivré relevant d'un schéma d'identification électronique qui figure sur la liste publiée par la Commission en vertu de l'article 9 ;

b) le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne dans le premier État membre, à condition que le niveau de garantie de ce moyen d'identification électronique corresponde au niveau de garantie substantiel ou élevé ;

c) l'organisme du secteur public concerné utilise le niveau de garantie substantiel ou élevé pour ce qui concerne l'accès à ce service en ligne. »

10 LA CRÉATION D'UN NOUVEL OBJET JURIDIQUE : LA SIGNATURE ÉLECTRONIQUE DE PERSONNE MORALE

Notre analyse

Autre nouveauté importante, ce règlement introduit un nouveau concept juridique – qui n'existait pas en droit Français – à savoir la signature de personne morale ou « cachet électronique ».

Jusqu'à présent, seules les personnes physiques pouvaient créer une signature électronique. Les entreprises, les administrations et les associations vont désormais pouvoir signer en leur nom des documents qui seront recevables comme preuve en justice. Là encore, le règlement distingue les services de cachets électroniques qualifiés des services non qualifiés. Comparable à un tampon électronique d'entreprise, le cachet électronique permettra de sceller électroniquement des documents et surtout de certifier leur provenance.

Extraits du règlement

« **Article 3**

Définitions

24) "créateur de cachet", une personne morale qui crée un cachet électronique ;

25) "cachet électronique", des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières ; »

« **Article 35**

Effets juridiques des cachets électroniques

1. L'effet juridique et la recevabilité d'un cachet électronique comme preuve en justice ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

2. Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

3. Un cachet électronique qualifié qui repose sur un certificat qualifié délivré dans un État membre est reconnu en tant que cachet électronique qualifié dans tous les autres États membres. »

11 L'HORODATAGE INTRODUIT AU NIVEAU EUROPÉEN

Extraits du règlement

« **Article 41**

Effet juridique des horodatages électroniques

1. L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

2. Un 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.

3. Un horodatage électronique qualifié délivré dans un État membre est reconnu en tant qu'horodatage électronique qualifié dans tous les États membres. »

Notre analyse

Alors que l'horodatage électronique bénéficie désormais d'un cadre juridique clair et mature en France grâce notamment au RGS, celui-ci n'avait jusqu'à présent pas été introduit en droit européen. C'est désormais chose faite puisque le règlement eIDAS définit à la fois l'horodatage et l'horodatage qualifié.

Rappelons qu'un horodatage garantit l'existence d'un fichier à une date donnée et que celui-ci n'a pas été modifié au bit près depuis cette date (principe d'intégrité). Dès lors, un document scellé avec un horodatage qualifié au sens européen bénéficiera d'une présomption de fiabilité quant à sa datation et son intégrité et ce devant toutes les juridictions européennes.

12 DE LA VALIDATION DE SIGNATURE ÉLECTRONIQUE

Notre analyse

Tous les textes juridiques qui ont été publiés jusqu'à présent accordaient une large place à la génération des certificats et à la création des signatures électroniques.

En revanche, ils abordaient assez peu la manière dont une signature doit être vérifiée et validée. Le règlement européen rectifie le tir en consacrant deux articles à la validation des signatures qualifiées.

L'article 32 liste les exigences applicables à la vérification d'une signature électronique qualifiée tandis que l'article 33 intronise un nouveau service de confiance dédié à la validation de signature électronique qualifiée.

À l'horizon 2016, on peut donc imaginer voir fleurir les services en ligne de vérification de signature électronique compatibles avec le nouveau règlement.

Extraits du règlement

« **Article 33**

Service de validation qualifié des signatures électroniques qualifiées

1. Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui:

a) fournit une validation en conformité avec l'article 32, paragraphe 1; et

b) permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables au service de validation qualifié visé au paragraphe 1. Le service de validation de signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

13 LA NOTION DE SERVICE DE CONSERVATION

Extraits du règlement

« **Article 34**

Service de conservation qualifié des signatures électroniques qualifiées

1. Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables au service de conservation qualifié des signatures électroniques qualifiées [...] »

Notre analyse

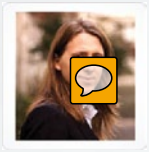
Dernière nouveauté à mentionner, la notion de conservation des signatures électroniques. En effet, le règlement est à ce jour le seul texte de loi à s'intéresser à la préservation de la fiabilité d'une signature électronique dans le temps. Il est en effet fondamental de pouvoir démontrer sur de très longues durées, l'intégrité et la valeur probatoire de tout document ayant été signé de manière cryptographique. C'est pourquoi l'article 34 définit un service de conservation qualifié des signatures électroniques qualifiées tout en se gardant bien d'utiliser le terme « archivage ».

La sémantique utilisée pour décrire ce service (i.e. extension de la fiabilité des signatures, période de validité technologique, etc.) semble faire référence aux formats « étendus » comme PAdES-LTV ou XAdES-A, qui permettent de prolonger la durée de validation d'une signature et de garantir la fiabilité d'une signature indépendamment de l'endroit où elle est archivée.

Sur ce point comme sur beaucoup d'autres, il est encore trop tôt pour savoir précisément en quoi consistera ce service. Il faudra attendre la publication des actes d'exécution qui eux-mêmes feront référence aux normes ETSI dans lesquelles on trouvera la manière d'implémenter tous ces nouveaux services !

À propos des auteurs

Julien Stern, CEO



Ancien élève de l'ENS de Lyon et titulaire d'un doctorat en cryptologie, Julien Stern est l'un des co-fondateurs de Cryptolog. Après avoir passé 8 ans en tant que CTO à bâtir l'offre de l'éditeur, il est aujourd'hui reconnu comme l'un des experts européens de la signature électronique. En 2009, il prend en charge la direction générale de Cryptolog et orchestre la mise sur orbite d'Universign, qui rencontre aujourd'hui un succès exceptionnel sur le marché Français.

Andréa Rock, ingénieur R&D, membre de l'ETSI

Titulaire d'un doctorat en cryptographie de l'Ecole Polytechnique réalisé à l'INRIA Paris-Rocquencourt, Andrea complète sa formation par un post-doctorat dans l'université Finlandaise d'Aalto dans le groupe cryptographique de Kaisa Nyberg. Après divers projets de recherche européens, elle rejoint Cryptolog en 2011 pour renforcer l'équipe R&D. Membre de l'ETSI et spécialiste des listes de confiance (TSL), elle est aujourd'hui rapporteur des standards CAdES et TS 119 101.

Sources

Lien vers le **communiqué du Conseil de l'Union Européenne** : Voir en ligne

Liens vers les **textes définitif** :

Conseil Européen : en français - en anglais

Lex Europa : en français - en anglais

Lien vers la **vidéo de la table ronde des Assises de la Confiance Numérique** : Voir en ligne

À propos de Universign

Universign est la plateforme Cloud de signature électronique, d'horodatage et de gestion des identités numériques de la société Cryptolog. Tiers de Confiance, Cryptolog est depuis plus de 15 ans un pure player de la confiance numérique.

Pour plus d'informations : www.universign.com

Nous vous remercions de l'attention portée à notre livre blanc dédié au nouveau règlement européen sur la signature électronique.

VOUS AVEZ UN PROJET ?

RENCONTRONS-NOUS !

01 44 08 73 00 - sales@universign.eu

universign

7, rue du Faubourg Poissonnière 75009 PARIS
+33 (0)1 44 08 73 00 - sales@universign.eu - www.universign.com