WAVESTONE

eIDAS

EN ROUTE VERS UNE EUROPE DE LA CONFIANCE NUMÉRIQUE

Le règlement européen eIDAS (electronic IDentification And trust Services) est entré en vigueur le 1er juillet 2016. L'objectif de ce règlement est « d'instaurer un climat de confiance dans l'environnement en ligne » en fournissant un cadre transnational et intersectoriel complet pour des transactions électroniques sûres, fiables et simplifiées entre citoyens et entreprises.

Il amène de nombreuses nouveautés par rapport à la précédente directive européenne de 1999/93/CE sur le cadre règlementaire lié à l'identification électronique et aux services de confiance. Ce climat de confiance couvre donc l'identification et l'authentification électroniques mais également d'autres services de confiance tels que l'horodatage ou encore le recommandé électronique. La mise en place d'un tel cadre permettra d'effectuer des démarches administratives dans tous les pays membres de l'Union Européenne et imposera la reconnaissance mutuelle.

Le texte met en lumière un des principaux problèmes rencontré aujourd'hui : « Dans la plupart des cas, les citoyens ne peuvent pas utiliser leur identification électronique pour s'authentifier dans un autre État membre parce que les systèmes nationaux d'identification électronique de leur pays ne sont pas reconnus dans d'autres États membres ». Cette non-reconnaissance est due à l'interprétation et à la mise en œuvre technique par chaque État membre de la directive, amenant ainsi à des problèmes d'interopérabilité et des divergences dans les contrôles effectués. Concernant les services de confiance tels que l'horodatage ou encore le cachet, les divergences émanent de l'absence de cadre juridique clair au niveau européen, ce qui constitue un réel frein au développement de la confiance numérique dans un contexte transfrontalier.

AUTEURS

FLORIAN FEUILLARD
florian.feuillard@wavestone.com

MATTHIEU GUILLAUME
matthieu.guillaume@wavestone.com

TÉMOIGNAGES

DIDIER LEFEVRE
DSI, CSN

YANNICK THOMASSIER
DSSI, Real.Not, opérateur de l'IGC du CSN

UN CADRE COMMUN

Bien que le règlement reprenne la majeure partie des dispositions de la directive qu'il abroge, il y apporte cependant quelques modifications, ainsi que des nouvelles dispositions, renforçant ainsi cette reconnaissance européenne des services de confiance. Le règlement détermine notamment :

- **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 ;
- **Les règles applicables aux services de confiance**, en particulier pour les transactions électroniques ;
- **Le cadre juridique pour les services** de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envois recommandés électroniques et de certificats pour l'authentification de site internet.

Contrairement à la directive 1999/93/CE, eIDAS est un règlement. **Il n'y a donc pas de transposition nationale**, le texte est applicable pour l'ensemble des États membres.

VERS UNE HARMONISATION EUROPÉENNE : LES POINTS CLÉS

Le règlement introduit un certain nombre de nouvelles notions, parmi lesquelles on peut noter :

- **L'acceptation du document électronique en tant que preuve devant la justice** ;
- **La création d'un label de confiance** pour un marché plus transparent ;
- L'encadrement des méthodes de validation de signatures qualifiées par le biais de prestataires de services de confiance ;
- Le service de conservation qualifié des signatures électroniques qualifiées, pour garantir la fiabilité des signatures et donc leur valeur dans le temps ;
- L'horodatage au niveau européen, permettant une reconnaissance de la datation et de l'intégrité de données numérique et donc de la validité juridique du document dans toute l'UE ;
- L'obligation pour les États membres de maintenir des listes de confiance des services et prestataires qualifiés et labélisés à disposition du grand public ;
- L'assouplissement de la signature sécurisée : reconnaissance de la signature créée à distance par un tiers de confiance au nom du signataire pour faciliter les usages en mobilité.

Parmi les autres points remarquables, nous pouvons citer l'apparition d'un **nouveau principe juridique : la signature électronique de personne morale**. Le cachet électronique permettra donc aux entreprises et administrations de signer électroniquement en leur nom des documents afin de certifier leur provenance. Concrètement, un juge français ne pourra pas refuser un cachet ou une signature électronique apposé par une entreprise italienne avec une solution allemande. Enfin, nous pouvons également souligner **l'introduction de la notion de signature qualifiée côté serveur**, ce qui permettra notamment le développement de nouvelles offres (en SaaS), objectif clairement affiché de ce nouveau règlement.

eIDAS définit par ailleurs une **graduation en 3 niveaux de signature de personne physique**, synthétisé dans le tableau ci-dessous, **contre 2 niveaux anciennement** pour la directive.

3 niveaux de signature de personne physique

VALEUR DE LA SIGNATURE (- → +)

	Signature simple	Signature avancée		Signature qualifiée	
Niveau de signature	Simple	Avancée LCP ETSI 319 411 Niveau LCP	Avancée QCP ETSI 319 411 Niveau QCP	Qualifiée QCP + QCSD ETSI 319 411 Niveau QCP + QCSD	
Niveau de certificat	Certificat simple	Certificat LCP	Certificat qualifié sur support logiciel	Certificat qualifié sur support matériel	
				Carte à puce	Serveur qualifié
Exigence enrôlement	Pas d'exigence	Identité vérifiée à distance	Identité vérifiée en face à face	Identité vérifiée en face à face (a) ou à distance (b) ou au moyen d'un certificat de signature électronique qualifié délivré conformément à (a) ou (b)	
Exigence dispositif de signature	Pas d'exigence	Pas d'exigence	Pas d'exigence	Dispositif de signature qualifié	
Bénéfice	Intégrité	Intégrité et non répudiation	Intégrité et non répudiation	Intégrité et non répudiation	

LCP : Lightweight Certificate Policy — QCP : Qualified Certificate Policy — QCSD : Qualified Signature Creation Device — : A définir

CONCRÈTEMENT, QU'EST-CE QUE CELA VA CHANGER ?

Un des premiers points notables concerne la mise en conformité en vue d'une qualification eIDAS pour les Prestataires de Services de Confiance (PSCO). Afin d'intégrer la liste des PSCO qualifiés (qui devra être publiée régulièrement) et donc reconnus par les États membres, ceux-ci devront respecter un ensemble d'exigences de sécurité (mesures techniques, organisationnelles, etc.) et notamment l'assurance de la vérification du lien entre l'identité d'un porteur et le certificat délivré. Pour cela, ils devront s'appuyer sur les standards décrivant les mesures de sécurité à mettre en place : analyse de risques, plan de cessation d'activité, processus de délivrance en face à face, notifications en cas d'atteinte à la sécurité, contrôles, responsabilités, etc. Ces mesures ne sont pas nouvelles en soit, le règlement définit seulement précisément ce qui est attendu dans chacun de ces chapitres en y ajoutant de nouvelles notions (exemple : « *The Trust Service Provider shall state in its practices the provisions made for termination of service* »). L'interopérabilité technique des systèmes passe donc par la revue des référentiels nationaux, comme le Référentiel Général de Sécurité (RGS) en France, et la coopération des pays membres.

Le texte va d'ailleurs dans ce sens en mettant en avant ce besoin de travail commun : « La coopération des États membres devrait faciliter l'interopérabilité technique des schémas d'identification électronique notifiés en vue de promouvoir un niveau élevé de confiance et de sécurité, adapté au degré de risque. L'échange d'informations et le partage des bonnes pratiques entre les États membres en vue de leur reconnaissance mutuelle devraient faciliter une telle coopération ».

Cependant, la qualification reste une démarche volontaire et un label de confiance UE sera créé pour identifier les PSCO qualifiés. Pour obtenir ce label, les prestataires de services de confiance devront se soumettre à des audits qui attesteront du respect des mesures définies dans les standards adossés au règlement. Il est donc fort probable que dans les mois qui viennent, les PSCO recherchant la qualification eIDAS lancent des projets globaux de mise en conformité comprenant la mise à jour documentaire (PC, DPC, PH, DPH, CGU, etc.), la revue de leur architecture d'IGC (Infrastructure de Gestion de Clés), de leurs gabarits de certificats, etc. À noter que les prestataires qualifiés dans le cadre de la directive restent qualifiés au sens du règlement jusqu'au renouvellement de leur qualification, mais devront passer un audit au plus tard avant le 1er juillet 2017 pour renouveler leur qualification. Ce délai de grâce ne devrait pas être superflu. Par exemple en France, le seul opérateur de qualification aujourd'hui officiellement accrédité ne l'est que depuis relativement peu de temps, ce qui a pu freiner le lancement de projets de mises en conformité.

L'EUROPE S'INTÉRESSE À L'ADOPTION DE CES TECHNOLOGIES DANS LES PAYS MEMBRES

Les autorités européennes, en particulier la direction générale de l'informatique (DG DIGIT) en charge des 4 piliers fondamentaux que sont l'eInvoicing, l'eDelivery, l'eSignature et l'eID, ont souhaité évaluer concrètement les forces en présence dans chaque pays. À ce titre, ils ont fait réaliser par Wavestone Luxembourg un sondage et organisé des groupes de travail à l'échelle européenne pour identifier les acteurs présents sur le marché et leurs besoins. Les différentes solutions pour stimuler l'adoption de chacun de ces piliers fondamentaux ont été analysées et discutées avec l'ensemble des acteurs. Résultats à venir !

Qualification eIDAS pour les services et les prestataires

RETOUR SUR UN PROJET DE MISE EN CONFORMITÉ

Le Conseil Supérieur du Notariat (CSN) est l'un des premiers acteurs français à entamer une démarche de mise en conformité avec le nouveau règlement eIDAS. En sa qualité de Prestataire de Services de Confiance, le CSN dispose d'une autorité de certification émettant notamment des certificats de signatures à destination des notaires pour la signature d'actes authentiques.

Rencontre avec Didier Lefèvre (DSI, CSN) et Yannick Thomassier (DSSI, Real.Not, opérateur de l'IGC du CSN).

Que pensez-vous de ce nouveau règlement ?

Yannick Thomassier : Avant ce règlement, il existait la directive 1999/93/CE mais un audit effectué dix ans après sa mise en place a mis en lumière ses limites. La réflexion initiée alors par la Commission au Parlement européen dans sa communication du 26 août 2010 (Une stratégie numérique pour l'Europe) est claire : « [...] la Commission a désigné la fragmentation du marché du numérique, le manque d'interopérabilité et l'augmentation de la cybercriminalité comme les principaux obstacles au cercle vertueux de l'économie numérique ». Le règlement européen veut remédier à certaines lacunes de la directive 1999/93/CE en imposant une même base légale à tous les États membres. Cependant le règlement n'a pas été pour le moment assorti de tous les actes d'exécution nécessaires à une transposition technique unique au sein de l'Europe. Chaque État membre doit donc décider de la façon dont il l'appliquera et ainsi fixer ses propres règles. Ceci correspond finalement au schéma d'implémentation que nous connaissons actuellement avec la directive 1999/93/CE.

En cela le règlement n'a pas encore complètement rempli ses promesses.

Didier Lefèvre : Néanmoins, une des vertus d'eIDAS est qu'il vise à établir une référence sur l'ensemble de la chaine de confiance. Ceci est une amélioration par rapport à la directive 1999/93/CE qui n'adressait qu'un spectre réduit, à savoir la signature électronique.

Pourquoi vous lancez-vous aujourd'hui dans cette mise en conformité eIDAS ?

YT : Nous sommes dans l'obligation de nous mettre en conformité dans la mesure où la signature des notaires est une signature qualifiée.

Quelles sont les opportunités que représente ce règlement pour vous ?

YT : Nous y voyons un intérêt pour le développement de la signature dans le Cloud. L'utilisation de la carte à puce pour signer des actes notariés est un premier pas vers la dématérialisation, mais celle-ci reste encore très contraignante. Or aujourd'hui, l'usage informatique ne se limite plus à un ordinateur, mais il inclut les smartphones, les tablettes, etc. Le notaire est de plus en plus mobile, et il doit être capable de signer via ces dispositifs afin de se démarquer et répondre aux besoins de ses clients. Le règlement eIDAS est une formidable opportunité d'offrir d'autres moyens de signature qualifiée.

W : Quelle est la principale difficulté que vous avez rencontrée ?

YT : Le planning. Nous avons opté pour une anticipation maximale de cette mise en conformité, car le changement est un processus fastidieux et très long : il faut compulser de nombreux documents, définir de nouveaux processus, mettre en œuvre parfois de nouveaux produits et faire concorder le tout dans un planning qui respecte les jalons fixés dans le règlement lui-même. D'autant plus qu'en tant que professionnel du droit, nous nous devons d'être prêts au bon moment.

Quels conseils donneriez-vous à ceux qui souhaiteraient se lancer dans un projet de conformité similaire ?

YT : Il y a principalement deux points sur lesquels il faut être vigilant. D'une part, il est nécessaire de faire preuve d'agilité face à un nouveau règlement, soumis à de potentielles évolutions. Le corpus documentaire technique français par exemple n'est pas encore figé. D'autre part il faut se mettre en ordre de marche assez rapidement afin de préparer l'audit de qualification dans de bonnes conditions.

Comment voyez-vous le futur concernant ce règlement européen ?

YT : L'implémentation technique du règlement eIDAS est sujette à l'interprétation de la part des organes de contrôle nationaux. Cela pourrait impacter son déploiement. Il pourrait donc il y avoir une phase 2 au règlement afin d'en clarifier l'implémentation et rendre ainsi son déploiement homogène au sein de l'Europe.

Et pour la suite ?

YT : Nous espérons obtenir notre qualification eIDAS dans les temps. Rendez-vous le 1er juillet 2017 !

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods). Il figure parmi les leaders indépendants du conseil en Europe.

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.