



Livre Blanc

Comprendre les signatures électroniques eIDAS

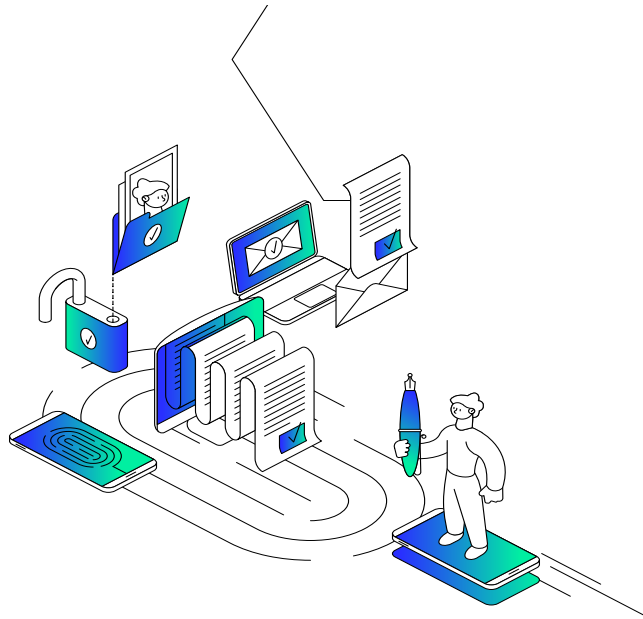
Sommaire

- 3** Introduction
- 4** Les exigences légales au sein de l'Union européenne
- 5** La valeur juridique des signatures électroniques
- 6** Les signatures simples, avancées et qualifiées : quelles différences ?
- 8** Quid du cachet électronique ?
- 9** Garantir l'interopérabilité des systèmes
- 10** Quelles sont les différences entre XAdES, PAdES et CAdES ?
- 12** Comprendre le mécanisme de création de la signature électronique
- 14** Développer un écosystème de signatures électroniques durable
- 16** À propos de COSI, plateforme de services de confiance certifiée eIDAS
- 17** À propos de LuxTrust

Introduction

La crise sanitaire et la généralisation du télétravail ont accéléré la digitalisation des documents et l'automatisation des processus des entreprises. Ce que les entreprises considéraient comme un moyen de maintenir leur niveau d'activités est maintenant perçu comme un levier de croissance et un moyen d'accroître leur productivité.

De plus en plus d'entreprises prévoient de mettre en œuvre des stratégies se reposant sur l'exploitation de technologies de pointe pour optimiser leurs processus actuels. La **signature électronique** est un de ces outils qui apporte de véritables avantages à une organisation.



Grâce à la signature électronique, la présence physique n'est plus requise pour signer les documents. La signature peut se faire de n'importe quel endroit et sur n'importe quel appareil utilisé, permettant aux signataires de se concentrer davantage sur des tâches à valeurs ajoutées.

La signature électronique fait également partie intégrante d'un parcours client entièrement numérique, créant une expérience positive dès les premières interactions avec les services d'une entreprise.

Enfin, le vrai avantage réside dans le fait que **la signature électronique contribue fortement à dissuader les tentatives de fraude**. En effet, une signature électronique sécurisée appliquée conformément aux exigences réglementaires (**règlement eIDAS** de l'Union Européenne) offre un niveau élevé de garantie sur l'identité du signataire. Cela permet également de détecter si le contenu du document a été modifié de quelque manière que ce soit après la signature.

L'objectif de ce document est de passer en revue les **différents types de signatures électroniques** réglementés au niveau de l'Union Européenne pour vous permettre d'utiliser la signature électronique de manière conforme et correcte afin de protéger vos documents.

Les exigences légales au sein de l'Union européenne

La nature même de la signature électronique, c'est-à-dire le fait de donner son approbation ou son accord sur certaines conditions, a des implications juridiques qui peuvent varier d'un pays à l'autre. Cela crée des problèmes de conformité et augmente les charges administratives et technologiques des entreprises opérant à l'échelle internationale.

En ce qui concerne la signature électronique au sein de l'Union européenne (UE), le Règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (le « **règlement eIDAS** »), est la référence clé. Entré en vigueur en 2016, le règlement eIDAS a créé un cadre juridique commun et normalisé pour que les signatures électroniques et les autres services de confiance soient reconnus et acceptés juridiquement dans tous les Etats membres de l'UE.

Grâce au règlement eIDAS, la signature électronique est reconnue comme preuve en cas de litige. **Aucun juge de l'UE ne peut refuser un document électronique comme preuve en justice au seul motif que sa signature se présente sous une forme électronique.**

De plus, en utilisant une signature électronique dite qualifiée, les entreprises et les particuliers peuvent ainsi signer électroniquement tout type de documents et contrats avec un effet juridique contraignant et les envoyer électroniquement sans craindre les disparités juridiques. La signature électronique permet d'échanger des biens et services sur le marché unique de manière plus simple, moins onéreuse et plus fiable que d'autres solutions.

La valeur juridique des signatures électroniques

Le règlement eIDAS définit et fixe les normes pour **trois types de signature électronique** visant à empêcher la falsification et la fraude et à offrir aux entreprises la flexibilité dont elles ont tant besoin. En ayant la possibilité de choisir la forme de signature électronique la plus adaptée à leurs besoins, les entreprises sont à même de trouver le bon équilibre entre l'expérience client et la conformité.

Lorsqu'on évalue les niveaux de signature électronique, il faut prendre en compte trois aspects essentiels :

- ▶ **l'authenticité**: la capacité à évaluer si l'identité du signataire est clairement connue ;
- ▶ **l'intégrité**: la capacité à vérifier si les données ont été modifiées après la signature ;
- ▶ **le consentement**: la capacité à prouver clairement que le signataire a donné son consentement sur le contenu du document.



Les signatures simples, avancées et qualifiées : quelles différences ?

1. La signature électronique

La plupart des gens de l'industrie parlent de la « signature électronique simple » bien que ce nom ne soit pas vraiment correct d'un point de vue juridique. **C'est la forme la plus élémentaire et la plus facile à utiliser.** Il peut s'agir d'une signature dessinée avec le doigt sur un écran tactile, d'une image numérisée de la signature manuscrite envoyée par e-mail ou la case à cocher utilisée pour accepter les conditions générales d'un site internet lors de la connexion au compte.

Elle ne requiert pas l'identification claire et incontestable du signataire avant ou pendant la signature. **En raison de son faible niveau de complexité technologique, elle peut également être facilement falsifiée.** Bien entendu, elle ne bénéficie pas d'un niveau élevé d'assurance. En cas de litige, elle doit être accompagnée par d'autres types de preuves.

2. La signature électronique avancée

Une signature électronique avancée est beaucoup plus stricte qu'une signature électronique simple. La signature électronique avancée est plus sûre et fiable que la signature simple puisqu'elle doit répondre aux exigences eIDAS spécifiques définies à l'article 26. La signature électronique avancée :

1. est liée au signataire de manière univoque ;
2. permet d'identifier le signataire ;
3. a été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son seul contrôle ; et
4. est liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

La signature avancée offre un degré plus élevé de sécurité et de confiance, car elle permet d'identifier le signataire. Les modifications apportées à un document après la signature sont détectées et affichées. Dans un tel scénario, la signature devient alors automatiquement invalide. Toutes ces exigences rendent ce type de signature difficile à rejeter devant les tribunaux. Ce format prévoit des dispositions de sécurité particulières en comparaison avec d'autres formats de signature permettant par exemple la conservation à long terme des signatures et des cachets électroniques, chose impossible pour de nombreux autres formats connus.

3. La signature électronique qualifiée

C'est la plus complexe de toutes les signatures et la seule dont l'effet juridique est équivalent à celui d'une signature manuscrite dans tous les États membres de l'UE. De plus, elle garantit l'identité du signataire avec un maximum de certitude. Au niveau technique, la signature électronique qualifiée est une signature électronique avancée qui satisfait deux exigences supplémentaires :

- A. La signature doit être créée sur la base de l'utilisation d'un **dispositif de création de signature reconnu comme qualifié**, qui doit satisfaire à des exigences de sécurité très strictes. Ce dispositif doit être évalué par un organisme compétent, puis certifié dans un état de l'UE. Si le dispositif est proposé en tant que service cloud, l'environnement d'hébergement doit également être évalué et certifié et le service lui-même doit être fourni uniquement par une autorité de confiance ayant le statut de **prestataire de services de confiance qualifié (PSCQ)** figurant dans **la liste de confiance européenne (EU Trusted List)**.
- B. La signature doit reposer sur **un certificat qualifié lié à l'identité du signataire**. L'identification du signataire est effectuée en **face-à-face**, par un PSCQ sous des conditions très strictes. Grâce aux nouvelles technologies, l'interaction en face-à-face peut être effectuée à distance depuis n'importe quel appareil (smartphone, tablette, PC), via **une identification vidéo**, à condition que le fournisseur soit certifié et reconnu par les autorités nationales compétentes. Cela est particulièrement utile pour les entreprises qui doivent enrôler et équiper des clients ou des collaborateurs d'un certificat qualifié à travers le monde.

L'ensemble des processus de vérification d'identité et d'accréditation en rapport avec la création d'une signature électronique qualifiée garantit le plus haut niveau de sécurité et de fiabilité. En cas de litige, sa validité est présumée et le principe du renversement de la charge de la preuve est appliqué, ce qui signifie qu'il appartient au demandeur de prouver que la signature n'est pas valide.



Quid du cachet électronique ?

Les entreprises et les institutions, comme les particuliers, doivent signer une grande variété de papiers officiels, mais parfois en grand nombre et de manière récurrente. Afin de répondre aux besoins spécifiques des entreprises, le règlement eIDAS introduit un concept juridique dédié exclusivement aux personnes morales : le cachet électronique.

Le cachet électronique atteste l'origine et certifie la fiabilité des données de l'entreprise. Contrairement à la signature électronique, il n'implique toutefois aucun engagement ni aucune obligation de la part de la société concernant le contenu du document tamponné, sauf celle de garantir son authenticité et son intégrité. En termes simples, **le cachet électronique est l'équivalent électronique du tampon traditionnel que les entreprises appliquent sur les documents papier.**

Le cachet électronique repose sur le même concept et la même technologie que la signature électronique. Par conséquent, ces deux notions partagent de nombreux points communs. Par exemple, les deux types de cachets électroniques - le cachet électronique avancé et le cachet électronique qualifié - doivent satisfaire aux mêmes exigences du règlement eIDAS sur la signature électronique avancée, respectivement la signature électronique qualifiée. Comme la signature électronique, le cachet électronique bénéficie également d'une reconnaissance et d'une acceptation juridiques communes dans tous les États membres de l'UE. En d'autres termes, il ne peut pas être refusé comme preuve en justice au seul motif qu'il se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences des cachets électroniques qualifiés, dont la validité est présumée. **A noter que, en Belgique, le cachet électronique qualifié a le même statut juridique qu'une signature électronique qualifiée, mais il n'est valable qu'entre entités belges.**

L'avantage distinct du cachet électronique sur la signature électronique est qu'il peut être exécuté à la fois manuellement et automatiquement. Grâce au cachet électronique, les entreprises peuvent signer de grands volumes de données, par exemple : les factures électroniques qui sont générées via un système comptable ; les modèles de contrat à partager avec plusieurs signataires ; les chèques de paie, etc..

Garantir l'interopérabilité des systèmes

L'intégration réussie d'une solution de signatures électroniques repose sur l'interopérabilité des systèmes, c'est-à-dire la capacité à se connecter et interagir avec des systèmes et solutions existants. Ceci peut être accompli en utilisant des pratiques et des normes de pointe qui garantissent que les documents signés électroniquement pourront être facilement consultés au-delà des frontières et en dépit de toutes les avancées technologiques possibles dans le temps.

Pour atteindre cet objectif d'interopérabilité, la Commission européenne a chargé **l'Institut européen des normes de télécommunications (ETSI)**, une organisation à but non lucratif, d'élaborer des normes techniques pour le cadre du règlement eIDAS. Il en a résulté la mise en place d'un écosystème complet pour créer et valider les signatures électroniques avancées et qualifiées. Ceci est obligatoire pour le secteur public de l'UE, mais le secteur privé l'adopte afin d'assurer la mise en place des solutions interopérables.

Les deux exemples les plus importants de normes syntaxiques adoptées pour coder les signatures électroniques avancées et qualifiées sont les **signatures électroniques avancées XML (XAdES)** et les **signatures électroniques avancées PDF (PAdES)**, que nous décrirons plus en détail dans la section suivante. Ces normes susmentionnées prévoient des dispositions permettant la validité à long terme des signatures et des cachets électroniques



Quelles sont les différences entre XAdES, PAdES et CAdES ?

XAdES

XAdES (XML Advanced Electronic Signatures) est codé dans un format textuel lisible conforme aux règles XML (Extensible Markup Language).

XAdES peut être utilisé pour signer tout type de document électronique, y compris les documents au format XML comme les transactions SEPA. Les autres types de documents incluent les images PNG ou JPEG, les fichiers multimédias, toutes les données binaires (telles que les fichiers .exe) et les documents PDF.

Plusieurs documents peuvent être regroupés logiquement et signés au moyen d'une seule XAdES. Grâce à ce format, deux signataires différents peuvent également signer le même document ou des groupes de documents en parallèle ou en séquence. Pour résumer, la signature XAdES peut être liée à un ou plusieurs documents signés, qui font ensuite partie d'une structure XML globale. Elle peut également être liée à un manifeste, les documents signés réels étant conservés ailleurs et séparément.

La signature XAdES est le choix idéal pour tous les cas d'utilisation commerciale, en particulier lorsque plusieurs documents doivent être signés en même temps ou lorsqu'un fort accent est mis sur les performances et le traitement automatique dans des structures de données personnalisées.

PAdES

PAdES (PDF Advanced Electronic Signatures) est plus restreint que la XAdES. Une structure PAdES est toujours intégrée au document PDF signé et ne peut être utilisée que pour signer un seul document PDF à la fois. Ce type de norme ne prend pas non plus en charge la signature parallèle.

La signature PAdES convient aux entreprises qui traitent uniquement des documents PDF et dans les situations où l'utilisation d'outils accessibles au public comme Adobe Reader est impérative pour valider les signatures électroniques. C'est généralement le cas lorsque les documents signés sont partagés avec un public général, c'est-à-dire dans un contexte entreprise à consommateur ou consommateur à consommateur.

La signature XAdES est plus puissante que la signature PAdES et permet de couvrir tous les cas d'utilisation de signatures PDF. Néanmoins, la motivation derrière une norme de signature spécifique pour les documents PDF a été alimentée par le fait que le PDF est un format très populaire, avec un support de création et de validation de signature intégré dans des outils Adobe comme Adobe Reader. Il n'est donc guère surprenant que la communauté Internet ait fortement préconisé l'extension d'un véritable support de signature PDF à une norme officielle.

CAdES

En plus de référencer ces deux principales normes, le règlement eIDAS, mettant en œuvre la décision de la Commission européenne, spécifie une norme générique supplémentaire élaborée par l'ETSI nommée CAdES (CMS Advanced Electronic Signatures). Elle propose des fonctionnalités très similaires à celles du format XAdES. CAdES peut être appliqué à n'importe quelle donnée binaire ou autre, mais il manque certains concepts clés XAdES comme la signature de manifeste ou la signature de documents multiples. CAdES n'offre donc pas d'avantage particulier par rapport au format XAdES. particular advantage over XAdES.





Comprendre le mécanisme de création de la signature électronique

Comme nous l'avons expliqué dans l'une des sections précédentes, pour qu'une signature électronique bénéficie d'un niveau d'assurance suffisant, elle doit être liée au signataire de manière univoque et permettre d'identifier le signataire qui contrôle les dispositifs de création de signatures. Outre ces exigences de base, la réglementation eIDAS exige une mise en œuvre spécifique pour la signature qualifiée. Le cadre juridique définit une mise en œuvre de référence basée sur un protocole d'infrastructure à clé publique (ICP) qui peut également être appliqué à la création de cachets électroniques

Conditions préalables à la signature

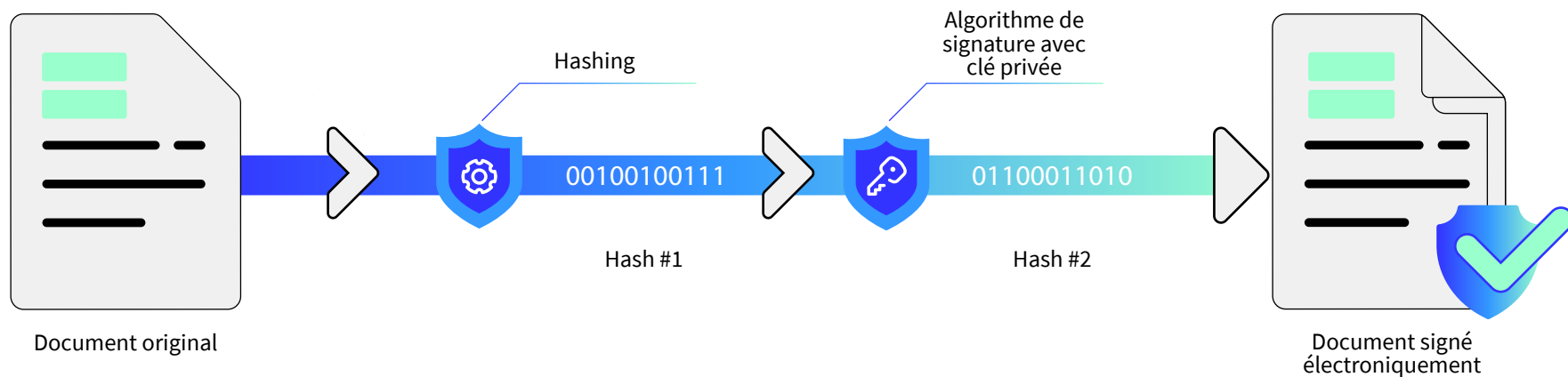
Le signataire possède une paire de clés cryptographiques qui sont étroitement liées entre elles. Les deux clés sont basées sur deux algorithmes cryptographiques utilisés en combinaison, à savoir **l'algorithme de synthèse** (« digest algorithm », également appelé algorithme de « hash ») et **l'algorithme de signature**. Une clé privée est conservée dans un dispositif protégé qui reste sous le contrôle exclusif du signataire ; l'autre clé est publique et peut être partagée avec n'importe qui.

Le dispositif protégé peut être une carte à puce ou tout autre dispositif matériel certifié, une application logicielle ou un service cloud pouvant être utilisé à distance par le signataire qui utilise un dispositif d'authentification local ou une application mobile. La divulgation ou le calcul de la clé privée, même en connaissant la clé publique, ne sont pas réalisables dans un délai réaliste.

Comment ça fonctionne ?

A partir du document qui doit être signé, un algorithme cryptographique dédié (« digest algorithm ») génère une courte chaîne de données en octets – c'est un code d'identification unique joint au document qu'on appelle « message digest » ou « hash ». Le signataire utilise alors sa clé privée pour appliquer l'algorithme de signature au résumé du message et à d'autres informations, créant ainsi la signature électronique. L'identité du signataire est ainsi liée au document représenté ou identifié par le « message digest ».

La validation fonctionne en appliquant un algorithme inverse. Le destinataire utilise sa clé publique sur une signature électronique pour le document électronique donné. Un résultat positif démontre que la signature n'a pas été modifiée et qu'elle ne peut avoir été créée que par le signataire en possession de la clé privée correspondante.



Mettre en œuvre un écosystème durable de signatures électroniques

La signature électronique d'un document ne se suffit pas à elle-même pour créer une solution pérenne. **Les entreprises doivent réfléchir à leurs besoins et au cycle de vie de leurs documents pour prendre en compte l'ensemble des pratiques et services qui améliorent la solution de signature électronique qu'elles ont choisie.**

Selon leurs cas d'usages et leur organisation, elles devront par exemple contrôler ou restreindre l'accès à certains documents numériques, organiser le partage des documents entre signataires ou adopter des systèmes qui offrent une vue d'ensemble claire aux signataires et enregistrent l'heure et la date de la signature

Il existe un large éventail d'éléments qui renforcent ou complètent la signature électronique pour aider les entreprises à gérer des risques ou des exigences plus particulières, tels quels : l'authentification forte du client, l'horodatage, la validation de signature électronique ou l'archivage numérique.

Des nombreux prestataires ne fournissent qu'une partie de ces services, ce qui peut créer des expériences cloisonnées pour les employés et les clients. Une plateforme unique qui centralise tous ces services, capable d'offrir une expérience utilisateur cohérente tout en garantissant la conformité aux réglementations en vigueur, est la solution idéale pour réussir à long terme grâce à la signature électronique. Une telle plateforme doit également englober des qualités plus pratiques, telles que la flexibilité, l'évolutivité et l'interopérabilité.

Ci-dessous, nous avons dressé une liste (non exhaustive) de questions à se poser avant d'adopter une solution de signature électronique dans votre organisation.

- Quelles sont les exigences ou les pratiques de votre secteur d'activité?
- **Quels types de documents doivent être signés électroniquement ?** Requièrent-ils tous le même niveau de signature électronique ?
- Qui sont les personnes qui signeront électroniquement ? Les signataires sont-ils déjà équipés d'un certificat (identité numérique) ?
- La solution de signature électronique vous permet-elle de signer tous les types de documents dont vous avez besoin?
- **Fournit-elle tous les types de signatures électroniques conformément à la réglementation eIDAS ?**
- **Est-elle compatible avec d'autres applications existantes** (intégrées ou pas) ? Prend-elle en charge d'autres fournisseurs d'identité numérique (itsme, FranceConnect ,etc.) ?
- Pouvez-vous la personnaliser ?
- La solution assure-t-elle la validation de la signature électronique ou la préservation à long terme?
- **Le fournisseur est-il un prestataire de confiance reconnu par l'UE ?**





À propos de COSI, la plateforme de services de confiance certifiée eIDAS de LuxTrust

Développée entièrement par LuxTrust, COSI est une plateforme innovante qui propose un écosystème numérique de confiance complet autour de la technologie de signature électronique pour accompagner les entreprises dans la numérisation de leurs processus et satisfaire aux exigences légales des autorités.

Grâce à COSI, les entreprises peuvent configurer leurs propres flux pour numériser et optimiser un large éventail de processus métier internes et externes, de la signature des rapports et des validations internes aux contrats multipartites. COSI prend en charge tous les niveaux de signature électronique eIDAS, jusqu'à un niveau qualifié, offrant aux entreprises une flexibilité accrue dans le choix de la solution la mieux adaptée à leurs besoins.

In addition to the creation of electronic signatures, COSI offers and facilitates the use of other eIDAS compliant solutions, such as:

1. La création de **cachets électroniques** permettant aux personnes morales de garantir l'intégrité et l'authenticité de leurs actifs numériques.
2. L'**horodatage** afin de bien enregistrer la date et heure d'une signature électronique.
3. La **validation des signatures électroniques** pour vérifier la validité des signatures électroniques fournies par d'autres fournisseurs.
4. La préservation à long terme pour augmenter la « durée de vie » d'une signature électrique.
5. L'**authentification forte** du client, jusqu'à l'identification à distance des utilisateurs finaux et enrôlement.
6. L'archivage numérique à valeur probante pour stocker des documents numériques pendant de plus longues périodes.

En intégrant le COSI, les entreprises obtiennent un point d'accès unique à la signature électronique et à ses services complémentaires en évitant ainsi de traiter avec un grand nombre de fournisseurs et de systèmes différents.

À propos de LuxTrust

Depuis plus de 17 ans, LuxTrust, principal fournisseur européen de services de confiance qualifié, équipe les clients et les entreprises en solutions numériques complètes et sur mesure pour numériser les processus et améliorer l'efficacité globale. Depuis sa création, LuxTrust a construit et maintenu un écosystème d'identité numérique à l'échelle nationale au cœur de l'Europe, fournissant des services d'identité numérique et de confiance à 99 % de la population luxembourgeoise et soutenant 95 % de la totalité des banques de détail opérant au Luxembourg.

LuxTrust est **un prestataire de services de confiance qualifié eIDAS** figurant sur la liste de confiance de l'UE et est **une Autorité de Certification**. Il offre toute la gamme de services de confiance qualifiés eIDAS disponibles sur le marché :

Identification des clients ou collaborateurs (en fournissant une identité numérique)

- Services d'authentification à des applications en ligne (bancaires ou autres)
- Services de signature électronique et de cachet électronique
- Service de validation de la signature électronique
- Service d'archivage à valeur probante
- Horodatage qualifié

En outre, LuxTrust propose des solutions pour se conformer à la directive DSP2, des certificats SSL et des solutions de collecte des données personnelles et de gestion de consentement.

Les solutions LuxTrust bénéficient du plus haut niveau de fiabilité et de confiance sur le marché. LuxTrust est supervisé et fait régulièrement l'objet d'audits et de contrôles obligatoires menés par des organismes de réglementation indépendants qui garantissent que les solutions restent conformes aux dernières réglementations européennes et du secteur.

- ▶ Une société robuste
- ▶ Une **gamme complète** de services eIDAS qualifiés
- ▶ Plus de **17 ans d'expérience** dans les services de confiance
- ▶ Un excellent suivi des projets livrés
- ▶ Statut **PSCQ** (Prestataire de services de confiance qualifié / Qualified Trust Services Provider)
- ▶ Signatures avancées et qualifiées à distance avec application mobile

Si vous souhaitez en savoir plus sur la signature électronique et les autres services de confiance, vous pouvez nous contacter par email : sales@luxtrust.com.

LuxTrust Luxembourg
IVY Building | 13-15, Parc d'Activités
L-8308 Capellen | Luxembourg

LuxTrust Belgique
54, Av. Louise
1050 Ixelles | Belgique

LuxTrust France
11, avenue Delcassé
75008 Paris | France

LuxTrust Monaco
Immeuble les Industries | 2 rue du Gabian
98000 | Monaco

sales@luxtrust.com
www.luxtrust.com

DISCLAIMER

Veuillez lire attentivement cette clause de non-responsabilité. Consultez des experts juridiques, techniques et financiers pour obtenir des conseils supplémentaires.

Les informations présentées dans ce livre blanc sont fournies à titre d'information uniquement et n'impliquent en aucun cas une relation contractuelle. Bien que les informations contenues dans ce livre blanc soient fournies de bonne foi et avec la meilleure interprétation de la législation actuelle, ces informations ne constituent en aucun cas un substitut à des conseils juridiques, commerciaux ou financiers et ne doivent pas être utilisées dans cet esprit. Bien que nous ayons fait tout notre possible pour nous assurer que les informations ont été obtenues à partir de sources fiables, LuxTrust ne garantit ni n'accepte la responsabilité de l'exactitude, de l'exhaustivité, de la validité, de l'actualité, de la fiabilité ou de la disponibilité de toute information. LuxTrust ne saurait être tenue responsable des résultats, dommages ou pertes que l'utilisation de ces informations pourrait entraîner.