# LES NOUVELLES TECHNOLOGIES DE L'ÉCONOMIE NUMÉRIQUE

*Par Eric Blot-Lefevre,*
*CERTIWAY Founder*
*NIS Expert European Commission*
*DG Connect Brussels*
*ebl@trustseed.com*

***Ce document est paru dans le numéro 105 de Signaux la revue d'ISEP Alumni, consacré à la « e-generation ».***

***Il est reproduit avec l'aimable autorisation d'ISEP Alumni.***

## INTRODUCTION

L'économie réelle est en train de basculer dans l'économie numérique. Il ne s'agit pas seulement du basculement des solutions informatiques *Off Line* installées sur un PC ou dans un centre informatique autonome, vers une solution *On Line* en SaaS et Cloud Computing où les moyens sont mutualisés, meilleur marché et plus sécurisés, mais il s'agit également d'une nouvelle architecture de communication associant des éléments fondamentaux de confiance numérique et de traçabilité qui puisse garantir la valeur juridique des correspondances documentaires et bancaires par Internet.

Autrement dit, la « commutation de messages » ne traite plus seulement la voix et les data avec des moyens de sécurité et d'interopérabilité. Elle traite également des fichiers documentaires signés dont il faut assurer d'abord la sécurité, la confidentialité et l'interopérabilité, mais aussi la valeur juridique avec un archivage légal de toutes les preuves de correspondance documentaire.

Le moteur du bouleversement est le nouveau business model de l'économie numérique[1]. Celle-ci a l'ambition de réduire de 70% le coût actuel[2] de la correspondance documentaire et bancaire, et de réduire de 70% les erreurs, les anomalies et les fraudes[3] qui représentent 200% du budget annuel de la

[1] *On estime que 60 % des entreprises fonctionneront en SaaS, IaaS et Cloud Computing d'ici 2017*
[2] *1000 Mrd par an en Europe selon SSEDIC DG Connect 2013*
[3] *1000 Mrd € par an en Europe*

Commission Européenne ! Combien de temps la démocratie peut-elle tenir avec plus de 1000 Mrd € de fraudes dont 65% sont internes à l'entreprise ?

En avril 1988, six mois après le premier crash financier, Alan Greenspan Gouverneur de la Federal Reserve USA, me fit la réflexion suivante : *L'application règlementaire de Bale 1 ne trouvera son efficacité qu'à partir du moment où les banques auront d'excellents outils informatiques de contrôle et de traçabilité, et décideront de faire de la sécurité un centre de profit à part entière. D'ici là, croyez-moi, l'Europe aura déjà sa monnaie unique !* Quelle clairvoyance et quelle lucidité !

Le moment est venu de croire aux excellents outils numériques, puisque l'économie numérique introduit un nouveau modèle d'architecture de sécurité et de confiance pour garantir sur Internet la vie privée, la valeur juridique des correspondances, leur interopérabilité et leur résilience universelle, ceci entre tous les réseaux communautaires qui se mettent en conformité avec ces nouveaux standards de communication et sous la surveillance des nouvelles Instances de Validation.

En d'autres termes, de même que pour la correspondance monétaire (numérique ou scripturale) il existe entre les Tiers de Confiance une obligation de résultat avec une instance supérieure de validation pour garantir la traçabilité des mouvements de monnaie électronique bilatéraux entre les personnes morales et physiques, il doit exister pour la correspondance documentaire la même obligation de résultat sur la bonne fin des opérations entre les prestataires de service documentaire et les parties en correspondance bilatérale, et les mêmes garanties provenant d'une instance de validation indépendante qui assure et administre la valeur juridique et l'interopérabilité des transactions numériques.

Dans le bilan numérique ou dématérialisé d'une entreprise, il n'y a pas de raison que les fichiers monétaires soient totalement certifiés à valeur probante, si pour leur contrepartie (les fichiers documentaires des transactions) il n'existe que des obligations de moyens comportant des trous dans la sécurité qui occasionneraient des erreurs, des anomalies et des fraudes. Comment les auditeurs dans les entreprises et les agences de notation peuvent ils se contenter de croire que les documents de bilans sont parfaits ?

L'enquête de PWC France (Février 2014) souligne que 45% des entreprises estiment que leurs données ne sont pas fiables. Mais entre deux fichiers, comment reconnait-on celui qui est original de celui qui ne l'est pas ? Dans son article (Le Monde), Marc Roche écrit : l'Administrateur chargé de la liquidation de Lehman Brothers (15 Mrd $ de pertes) se plaint d'avoir à *déterminer les vrais propriétaires des avoirs et des créances* et que cette recherche *revient à dévider toujours plus avant la pelote d'un incroyable enchevêtrement* ! Les grandes fraudes sont à l'origine de toutes les crises financières à l'échelle des nations et du monde : plus de 500 Mrd $ de fraudes financières entre 2000 et 2012.

La majorité des fraudes dans les entreprises se font en altérant la destination finale des documents conservés sur un serveur, en outrepassant les pouvoirs conférés par l'entreprise et en usurpant les identités numériques des contrôleurs de gestion. Avec les nouvelles technologies, les fraudes de paiements sont un nouveau registre de détournement de fonds, comme le précise FIA-NET. Selon le spécialiste de la sécurité du e-commerce, les tentatives de fraude à la carte bancaire ont représenté en 2012 près de 2,9% des 26 millions de transactions sur Internet en France. Le total de ces tentatives atteindrait 1,7 Mrd € sur les 45 Mrd € de chiffre d'affaires réalisé par le commerce en ligne français en 2012, soit une part de 3,91% en valeur. Les tentatives réussies (1 sur 30) ont finalement rapporté 80 millions d'euros aux cyber-escrocs. Il faut savoir que les trois premiers pays dans le palmarès des fraudes et de la cybercriminalité sont dans l'ordre les États-Unis, le Brésil et la France.

Mais grâce au relèvement des niveaux de sécurité et les standards pour les services de confiance en Cloud Computing, on peut envisager une réduction de ces phénomènes qui sont très liés aux échanges hybrides papier et fichiers non sécurisés. La politique de l'ENISA permet d'envisager sérieusement une réduction des fraudes avec les nouvelles architectures de sécurité et de confiance en Cloud Computing.

Avec un montant de 111 Mrd $ en 2012, le marché du Cloud Computing est estimé à 150 Mrd $ en 2014. C'est une croissance de 20 % comparable à celle des années 2006-2012 dans le BPO (Business Process Outsourcing) qui fut la première vague d'externalisation des applications de gestion des entreprises.

Le marché des services (SaaS et IaaS) en Cloud Computing atteint 677 Mrd de dollars en 2013. Pour Viviane Reding Commissaire Européen, le Cloud avec ses services numériques représente une création de 2,5 millions d'emplois et une contribution de 1% au produit intérieur brut européen.

Pour comprendre l'enjeu de l'économie numérique et de ses applications technologiques, il est utile de connaître l'ampleur des opérations concernées. Il existe en Europe environ 24 millions d'entreprises qui échangent avec les banques 60 milliards de transactions et 20 milliards de paiements règlementés. Le prix moyen de transaction papier actuel 1,32 € sera dans l'économie numérique descendu à moins de 77 centimes, soit une réduction de 70%, avec des niveaux de prévention et de sécurité 3 fois supérieurs à la situation actuelle.

Si on se base sur la valeur des transactions et des paiements en Europe qui est de 50.000 Mrd € en Europe, cela représente pour 80 milliards d'opérations au coût unitaire de 77 centimes (61,60 Mrd €) un prélèvement sur la valeur des transactions de 0,12 %.

Cette réduction des coûts est à la portée des marchands ou des portails commerciaux dans la mesure où la réforme des paiements (SEPA) autorise de nouveaux organismes non bancaires (Payment Service Providers) à exécuter des prélèvements automatiques en s'affranchissant des plateformes traditionnelles

Visa, Master Card, American Express… dont les services sont différents, plus onéreux et moins sécurisés dans le contexte de la réforme des architectures de sécurité et de confiance numérique.

On devine les bouleversements dans le domaine des « m.payment » : Juniper Research a signalé que plus de 1000 Mrd $ avaient déjà été exécutés dans ce nouveau contexte règlementaire.

Le développement des *marchés organisés* engagés dans l'économie réelle, des marchés électroniques tels que Swift, Clearstream, Euronext, … se métamorphose avec les nouvelles architectures de sécurité, les nouveaux standards et les nouvelles législations de la confiance numérique, afin de réduire drastiquement les litiges ou les contentieux par des mesures préventives sur Internet, et par voie de conséquence, la saisine des tribunaux totalement engorgés.

Une diminution de 80% des litiges par les *marchés organisés* permettrait d'alléger les budgets actuels de contentieux dont la croissance est inquiétante dans les entreprises, pour les États et pour les Compagnies d'Assurances. Il n'est plus rare de voir dans les entreprises un budget de contentieux supérieur au budget de recherche et développement !

Le projet de Directive NIS (Europe) trouve ici tout son sens puisqu'il s'agit d'introduire très rapidement dans les entreprises et les banques des contraintes fortes de Risk Management pour les échanges documentaires numériques à l'instar des correspondances bancaires armées par des mesures de risques et de contrôles règlementaires.

Les entreprises et les prestataires de services de confiance numérique devront appliquer des méthodes et des mesures de risk management dont les résultats seront communiqués à une instance de validation et de régulation accréditant chaque organisme de confiance, mesurant leur besoin en fonds propres en fonction des risques de leur activité, et transmettant certaines informations sensibles aux agences de cybercriminalité.

L'avenir de la technologie de sécurité et des tiers de confiance qui en font usage dépend donc des contraintes de cette Directive NIS et des Instances de validation qui n'accréditeront que les prestataires de service Internet qui s'y conforment, avec les fonds propres indispensables. La sécurité offerte aux Prestataires de Services de Confiance numérique par les hébergeurs et par leurs Data Centers Tier 4 sera également une donnée fondamentale qui entrera en ligne de compte dans la qualité des services garantis à la clientèle des entreprises et des particuliers. Il s'agit du Service Level Agreement (SLA).

On notera que le Grand Duché du Luxembourg, fort de son expérience trentenaire dans la création des « marchés organisés » financiers, a déjà pris une avance considérable dans l'équipement en data center Tier 4 des services de certification et de validation de ces nouveaux acteurs de confiance numérique, et dans la protection ou la défense de la propriété industrielle afférant à ces nouvelles technologies Internet.

Voici maintenant les principales priorités et propositions que nous avons fait entériner ou valider à la DG Connect dans le cadre des Commissions SSEDIC et NIS.

Ces propositions permettront les évolutions technologiques dans le contexte des besoins et des priorités des entreprises et des particuliers. Elles s'appliqueront aussi dans le contexte des réformes du droit face à la dématérialisation des signatures et des documents qui passent d'un support carte d'identité et papier à des supports en fichiers PDF, XML, EDI utilisant des moyens de scellement et d'horodatage numériques.

La réforme du droit et de la législation nationale concerne aussi les problèmes posés par la domiciliation des opérations qui sont réalisées par l'intermédiaire des prestataires de services de confiance en SaaS, IaaS et Cloud Computing. Ces prestataires peuvent être localisés à l'étranger et poser à leurs clients des problèmes de territorialité (conflit de juridiction).

Les propositions portent sur les priorités de la sécurité et de la confiance numérique :

1. La signature *on line* à la demande (SaaS et Cloud)
2. La spécialisation des opérateurs numériques dans les réseaux de confiance numérique
3. Le business model des identités numériques

## LA SIGNATURE *ON LINE* À LA DEMANDE

Le but est de remplacer la signature *off line* installée sur le poste de travail, compliquée à mettre en œuvre avec les parties en correspondance, avec des formats de fichiers sécurisés par des protocoles de communications spécifiques, avec des conventions inter-change contraignantes, et avec des listes de révocation nombreuses.

Ceci se fait en proposant aux usagers une solution de signature juridique *on line* « adoptive », plus conforme aux contraintes réglementaires et aux normes de sécurité, en associant tous les services d'un ou de plusieurs opérateurs affiliés à un Prestataire de services de Validation.

Les opérateurs préparent les documents à signer et assurent dans la signature juridique la complétude nécessaire à sa valeur juridique en établissant de bout en bout dans le Cloud la valeur probante du certificat de signature juridique, l'intégrité et la conformité du document ainsi que la manifestation du consentement du signataire pour une intention de gestion et avec les habilitations nécessaires à chaque type de document de correspondance.

Le prestataire de validation dans cette offre en SaaS assure, en toute indépendance par rapport aux opérateurs mandatés par les parties en correspondance, la tenue des listes de révocation, le référentiel documentaire comprenant les procédures et les fiches de traçabilité nécessaires aux contrôles de la valeur juridique (légalité, comptabilité, conformité), la liste des opérateurs de correspondance documentaire, la liste des autorités de certification de signature électronique qualifiée ou d'horodatage (ex. horloge atomique de Meudon) utilisées par les usagers (serveurs) ou leurs mandants, et la liste des bureaux d'enregistrement des identités numériques accrédités.

## LA SPÉCIALISATION DES OPÉRATEURS NUMÉRIQUES DANS LES RÉSEAUX DE CONFIANCE NUMÉRIQUE :

Il est indispensable pour la sécurité et l'interopérabilité des réseaux de confiance numérique de respecter les contraintes suivantes :

- **Les bureaux d'enregistrement en ligne des identités numériques doivent pouvoir créer des certificats d'identité numérique à valeur probante, sans utiliser de papier ni engager de démarche au comptoir.**

Chaque personne enregistrée doit pouvoir créer plusieurs identités numériques en fonction des attributs de confiance qui sont, soit spécifiés dans les relations bilatérales, soit prescrits dans les relations multilatérales, notamment au niveau des communautés d'intérêt, des nations ou des administrations.

Certains certificats d'identité numérique doivent pouvoir être mesurés sur le plan juridique à partir des justificatifs produits en ligne par les déclarants, ou en fonction de leur reconnaissance préexistante par des bureaux d'enregistrements préétablis et respectant la charte de notation de la valeur juridique des identités numériques établie par l'instance de validation dont ils dépendent.

La reconnaissance mutuelle des niveaux de valeur probante des identités numériques permet à un souscripteur d'identité numérique de s'inscrire et d'être reconnu plus rapidement si une autre communauté l'a déjà inscrit et a passé une convention d'équivalence des identités numériques avec une communauté partenaire.

- **Les opérateurs doivent pouvoir se spécialiser dans la préparation des signatures documentaires et dans l'exécution des services documentaires auxiliaires, comme l'archivage ou la gestion des comptes.**

La préparation des signatures documentaires est soumise à des contraintes très fortes de consultation préalable des Prestataires de Validation pour se conformer à la situation des listes de révocation, des référentiels documentaires et des listes d'opérateurs mandatés par les parties en correspondance.

Ces contrôles de conformité et d'interopérabilité entre les opérateurs affilés aux réseaux de confiance numérique sont des mesures préventives indispensables avant de lancer l'émission des correspondances documentaires, et pour finalement garantir leur valeur juridique dans l'exécution des services de back-office. Les tiers d'archivage ne sont pas autorisés à conserver des documents avec leurs preuves de correspondance sans être assurés de leur valeur juridique pour l'archivage légal.

- **Les opérateurs documentaires de signature juridique à la demande fonctionnent en interopérabilité pour leurs clients.**

Ils fonctionnent, d'une part avec leurs agents d'authentification forte mandatés pour les reconnaître et pour protéger leurs informations secrètes et d'autre part, avec les prestataires de services spécialisés dans la gestion confidentielle des documents après la phase de signature (back-office).

Les opérateurs qui assistent les parties en correspondance dans leur signature juridique ne sont pas autorisés à garder les données de signature, mais uniquement leur fiche de traçabilité.

Pour le back-office, il s'agit notamment des spécialistes mandatés pour l'archivage, la commutation de messages, les transferts de fichiers sécurisés, le routage des emails, des fax ou des courriers hybrides envoyés par la poste.

Pour assurer l'interopérabilité instantanée, les prestataires de validation développeront, comme les banques, des solutions de domiciliation de compte documentaire sur un modèle standard.

**Toutes ces dispositions sont prévues dans le projet de Règlement venant se substituer à la Directive actuelle des services, et dans les aménagements et nouveaux usages de signature juridique en ligne.**

La standardisation des procédures et des formats de traçabilité et d'interopérabilité est nécessaire au niveau de l'organisation des prestataires de validation pour assurer en temps réel le contrôle des listes de révocation, la mesure de la valeur probante des correspondances, l'instantanéité des échanges de données sécurisées entre les opérateurs, l'instantanéité de leurs communications avec les instances de validation, la consultation des autorités de certification garantes des signatures électroniques et des marques de temps, et enfin pour garantir en fonction des incidents la résilience par l'analyse systématique

des anomalies relevées sur les fiches de traçabilité circulant entre les opérateurs dans le Cloud (sur toute la chaine de confiance en Cloud Computing).

La résilience permet d'engager les mesures correctives et de transmettre les déclarations *ad-hoc* aux instances supérieures de surveillance et de régulation (cybercriminalité, défense professionnelle, autorités de marchés).

## LE BUSINESS MODEL DES IDENTITÉS NUMÉRIQUES

- **Il existe trois secteurs d'activité rémunérés dans l'économie numérique :**
  1. L'acte de signature off line ou on line en SaaS et Cloud Computing
  2. La création d'identités numériques sans papier et avec la mesure dynamique de la valeur juridique de leur certificat d'identité en fonction de nombreux critères convenus, soit sur un plan légal, soit sur un plan conventionnel.
  3. La création des conventions inter-change signées et de nature commerciale ou financière, qui stipulent entre les parties leurs attributs de confiance pour leurs identités numériques et leurs signataires (fondés de pouvoirs), les types de correspondance autorisés avec leurs procédures spécifiques, et les opérateurs documentaires choisis par les parties pour chaque type de correspondance avec leurs adresses de domiciliation (Data Center, SaaS, Cloud Computing).

- **La tarification des signatures numériques :**

La tarification se fait par un abonnement qui revient à 20/80 centimes par signature selon la qualité des services rendus. Il est probable que le prix baissera rapidement pour toutes les signatures qui ne couvrent pas tous les domaines de correspondance (transactions, paiements, courriers, contrats) et qui ne délivrent pas sur un ordinateur personnel ou sur un téléphone mobile toutes les assurances de valeur probante et d'interopérabilité nécessaires aux parties en correspondance dans tous les pays du monde.

- **La création des identités numériques :**

C'est un domaine très lucratif si le bureau d'enregistrement est capable de gérer pour chaque personne morale ou physique des identités multi critères et multi communautés avec une notation dynamique de la valeur probante, toujours en liaison avec un ou plusieurs prestataires de validation. L'identité numérique étant la racine de la valeur probante pour la signature documentaire et pour l'archivage légal, elle est essentielle aux quatre composants de la correspondance et de la confiance numérique : le document, la signature personnelle, les conventions commerciales et financières (obligatoires) et les mandats (mandats de délégation de pouvoir et mandats confiés aux opérateurs en SaaS).

On peut estimer que le prix minimum d'une identité numérique à valeur probante notée par une instance de validation pour réaliser des actes de commerce et de banque est de l'ordre de 6 € par an. Il y en a plus de 500 millions répertoriées pour les citoyens européens, chiffre auquel il faut ajouter les employés fondés de pouvoir (200 millions), et les identités des partenaires étrangers (import/export 80 millions). La qualité des identités numériques est un élément essentiel à la mise en œuvre par les opérateurs de contrats de services de qualité irréprochable : les SLA (Service Level Agreement).

- **La création des conventions inter-change nécessaires aux utilisateurs pour légaliser leurs relations commerciales, financières et bancaires.**

Cette demande viendra des marchands et des banques en ligne qui n'ont pas le savoir-faire mais qui doivent nécessairement établir ce genre de conventions signées pour leur activité.

L'exemple de la contrainte règlementaire du SEPA (qui impose à partir du 15 Février 2014 la signature en ligne des contrats de mandats de prélèvement automatique bancaire) illustre bien l'ampleur de cette application (15 Mrd de mandats numériques se référant à une convention commerciale et financière entre les marchands, leurs clients et les banques).

La convention inter-change signée indispensable dans les relations commerciales et financières est un véhicule intelligent et agile qui doit organiser tous les processus opérationnels en fonction des modalités d'échanges documentaires convenues entre les parties.

Les services de cette qualité, reposant sur des identités numériques très fortes et des procédés d'authentification également forts, seront encore plus rémunérés par le marché, puisqu'ils procurent les assurances en matière de valeur juridique et d'interopérabilité multi nationale et multi communautaire.

On estime que les bureaux d'enregistrement des identités numériques qui sont capables d'ajouter à leur service la signature des conventions bilatérales ou communautaires mentionnant les attributs de confiance choisies par les parties et les modalités de leur correspondance documentaire, pourront facturer plus de 20 € chaque convention inter-change en assurant son cycle de vie avec une instance de validation ainsi que les fonctions obligatoires de gestion des révocations et modifications.

- **L'authentification forte, nouveaux standards de valeur probante et d'interopérabilité, et la protection des secrets professionnels ou individuels :**

Le basculement des fonctions de gestion dans un environnement en SaaS et Cloud Computing va permettre d'utiliser l'ordinateur personnel ou son téléphone mobile comme une télécommande, pour réaliser les opérations dans un data center sécurisé Tier 4.

L'externalisation des opérations se concrétise par la création d'un bureau privé de correspondance dans un data center et par des mandats confiés aux opérateurs pour tous types de services de préparation et de signature juridique des documents de correspondance nécessaires au courrier, aux contrats, aux transactions ou aux paiements et autres instruments financiers.

Il résulte de ce nouveau modèle informatique et économique une obligation d'authentification très forte pour accéder au data center qui protège de compte documentaire et le secret documentaire. Les systèmes d'authentification forte par carte 3D Secure (SMS) ou 3 DSA (Signal audio crypté) sont indispensables.

De même, la protection des secrets personnels impose une séparation entre les agents d'authentification qui conservent les *credentials* et certains attributs de confiance réservés au secret professionnel ou individuel, et les autres opérateurs documentaires ou bancaires.

Enfin, les opérateurs documentaires qui préparent les spécimens documentaires avec les signatures apposées, devront systématiquement détruire leur spécimen dès qu'ils l'auront dupliqué, en fonction du nombre d'originaux et de copies de documents qui sont sous-traités, déposés, conservés et protégés par des opérateurs spécialement mandatés et organisés pour chiffrer les documents conservés en back-office .

## CONCLUSION : L'ÉCOSYSTÈME NUMÉRIQUE

Pour que le marché des correspondances documentaires signées, qui représente actuellement une charge globale pour les citoyens et les entreprises de 1000 Mrd € par an, économise 700 Mrd € (70%) grâce à la numérisation (Cf. Rapports de la Commission Européenne sur les factures et les paiements), il faut introduire chez les opérateurs actuels les niveaux nécessaires de sécurité et de valeur probante pour les identités numériques et pour leurs produits dérivés : documents, signatures, conventions inter change et mandats.

Il est aussi nécessaire d'introduire dans les réseaux de confiance numérique les instances de validation pour garantir les niveaux de valeur juridique et d'interopérabilité qui sont imposés pour les bilans comptables et digitaux des entreprises, par les autorités de marché et par les services de contrôles nationaux ou européens (Tracfin, Douanes, Cyber Criminalité Internationale…).

On estime que la création de valeur des niveaux de sécurité, de valeur juridique, d'interopérabilité et de résilience représente un marché de 25 Mrd €/an pour les éditeurs et acteurs en SaaS et Cloud Computing, et de 35 Mrd €/an pour les nombreuses instances de validation et de régulation des marchés.

Les solutions en SaaS pour les citoyens seront gratuites dans la mesure où ce sont les entreprises qui payent la sécurité et la valeur probante pour leur bilan comptable et financier : Digital Balance Sheet. Les citoyens ne paieront que leur besoin d'archivage légal et certaines mesures de confidentialité propres au secret individuel.

Ces solutions en SaaS seront « adoptives », c'est-à-dire faciles à utiliser, homogènes ou universelles pour fonctionner avec tous types de correspondances. Elles seront très bon marché, collaboratives, flexibles, compatibles (avec les applications logicielles existantes) et d'exécution instantanée. Ces solutions sont une simple *added value* facile à intégrer dans les applications des éditeurs de gestion documentaire.

La signature *on line* sera utilisée conjointement avec les signatures électroniques qualifiées qui sont davantage réservées à l'usage des serveurs d'entreprises ou des *administrés* (relations univoques avec les Administrations).

Les serveurs d'entreprises, qui envoient aux opérateurs des flux de fichiers en masse, utilisent la signature électronique. Enfin les opérateurs spécialisés, qui sont mandatés par leurs clients pour traiter le scellement de leurs fichiers, utilisent une signature électronique.

Le scellement des fichiers professionnels avec une signature électronique qualifiée, surtout quand il s'agit d'ordres de correspondance en masse (exemple 1 millions de correspondances bilatérales mettant en jeu 1 million d'identités numériques partenaires affiliées à de nombreux opérateurs distants) est une opération difficile dans la mesure où il faut respecter leurs contraintes règlementaires ou conventionnelles en concertation avec une ou plusieurs Instances de validation.

Ces mesures préventives pour assurer instantanément la sécurité et la légalité des transactions documentaires en préparation, complexifient l'émission des documents. La valeur probante de ces fichiers documentaires (PDF + XML) soumis à la signature électronique pour assurer leur intégrité, est subordonnée à la consultation préalable des services de l'instance validation (listes de révocation, référentiels documentaires, domiciliation des opérateurs, autorités de certification), afin d'éviter des erreurs de fabrication, l'invalidité des documents et l'archivage durable de documents sans valeur juridique ou exposés à des risques de contestation ultérieurement.

## GLOSSAIRE

| | |
|---|---|
| Bale 1 | Un ensemble de recommandations formulées en 1988 par un comité de banquiers, pour assurer la stabilité du système bancaire international. |
| BPO | Business Process Outsourcing |
| ENISA | European Network and Information Security Agency |
| NIS | Network Information Security |
| SEPA | Single European Payment Agreement |
| SLA | Service Level Agreement |
| SSEDIC | Scoping Single European Digital Identity Community |
| TDL | Trust in Digital Life |
| VAR's | Value At Risk |

## A PROPOS DE L'AUTEUR

**Eric Blot-Lefevre** est Fondateur, PDG, Administrateur des sociétés cotées éditeurs de progiciels de trésorerie pour les entreprises et les banques CONCEPT, XRT (Sage), Kyriba.com.

Ancien Directeur général de BATIF BANQUE, Directeur Central du CREDIT LYONNAIS, Directeur de la Trésorerie Centrale ALM des Groupes L'OREAL, Thomson Sa, THALES, Crédit Lyonnais Capital Markets. Ancien Président Directeur Général de DACF (Services de Comptabilité Fiducial), ancien administrateur de la SICOVAM/EURONEXT, Staff (Matif), ancien Président d'ECE Electronic Commerce Europe. Président de TrustSeed SAS. Fondateur de Certiway Luxembourg. Expert Délégué officiel des commissions « Scoping Single European Digital Identity Community" (SSEDIC) and NIS Network Information Security / DG CONNECT European Commission Brussels (Cyber Security / Criminality).

Avec Jean-Pierre Roumilhac, Eric Blot-Lefevre est co-auteur de l'ouvrage **Les échanges en toute confiance sur Internet** *(Éditions d'Organisation – 2003)*