Certigna

Vos parcours digitaux en toute confiance

Livre blanc

Signature électronique : 5 bonnes raisons de la déployer dans tous vos parcours !

En collaboration avec Archimag

Certigna

Vos parcours digitaux
en toute confiance

Une marque du groupe Tessi

Préface

.01 La signature électronique : véritable rempart à la fraude

1. La fraude sous toutes ses formes
2. Bien identifier les risques
3. Sécurité et expérience client : trouver le bon équilibre

.02 La signature électronique : tout savoir, tout comprendre !

1. Accélérer la souscription digitale
2. Sécuriser l'acte de signature numérique
3. Couvrir tous les usages, même en interne
4. Signer : avant tout une expérience utilisateur
5. Dépasser l'usage de la signature !

.03 5 bons conseils pour choisir son outil de signature électronique !

Et après ?

De la signature électronique à l'identité numérique

Préface

À l'heure où le numérique rythme les échanges, l'essor des nouvelles technologies et des outils de communication numérique transforme vos parcours clients et optimise les processus internes au sein de vos organisations. Cette révolution, bien que porteuse d'efficacité, engendre également de nouveaux risques qu'il devient impératif d'identifier et d'anticiper pour mieux s'en prémunir. De la fraude à l'identité à la cyberattaque, chaque étape du parcours est exposée à un risque d'intensité variable. Ainsi, le défi qui se pose à nous consiste à choisir les meilleurs outils pour contrer ces menaces émergentes et les anticiper avec pertinence.

C'est le cas de la signature électronique. Elle est plébiscitée par les entreprises et administrations et devient le maillon essentiel d'une souscription 100 % digitale. Clé d'une efficacité accrue, la signature électronique est désormais un outil indispensable dans la transition vers des parcours plus fluides et plus sécurisés. S'équiper d'un outil de signature électronique doit se penser à l'échelle de votre organisation afin de la déployer dans tous les processus impliquant un acte de signature. Par conséquent, les usages se démultiplient, en interne comme en externe, sur des opérations plus ou moins sensibles et impliquant différentes parties prenantes.

C'est pourquoi, dans ce livre blanc, nous explorons ensemble les raisons pour lesquelles le déploiement de la signature électronique s'impose dans toutes les facettes de vos parcours client et processus métiers.

Bonne lecture

Clément Savoie,
Directeur activité Confiance Numérique
Innovation&trust, la digital factory de Tessi

des organisations ont accéléré l'adoption de **la signature électronique** suite à la crise du COVID.

70%

des adultes ont renoncé à effectuer des **démarches administratives en ligne** en raison de la complexité des processus.

32%

87%

des Français ont déjà utilisé **la signature électronique.**

48%

des organisations indiquent que **la signature électronique** accélère la validation du contrat.

Source :
Ipsos Digital enquête 2023 | Etude Archimag

La signature électronique : véritable rempart à la fraude

1. La fraude sous toutes ses formes

La fraude en ligne a augmenté de façon spectaculaire au cours de la dernière décennie. Alors qu'en 2010 les pertes étaient estimées à environ **4 milliards de dollars** dans le monde, elles ont atteint plus de **42 milliards de dollars en 2020.** Une augmentation de plus **de 1000 %** ! À eux seuls, les services financiers représentent plus de 50 % des fraudes en ligne, suivis du commerce de détail et du e-commerce, particulièrement exposés au vol de données personnelles et financières.

Protéger son **identité numérique** est ainsi devenue un enjeu crucial aujourd'hui.
La fraude à l'identité en ligne se produit lorsque des individus utilisent frauduleusement les informations d'identification d'une autre personne pour effectuer des transactions ou accéder à des comptes en ligne. Les fraudeurs peuvent utiliser différentes techniques pour récupérer les données personnelles :

- Phishing ; vol de coordonnées bancaires via de faux emails portant le label d'organisations de confiance.
- Skimming ; logiciels installés sur des terminaux de paiement pour collecter les données des cartes de crédit.
- Attaques en ligne ; logiciels malveillants de type malware ou spyware installés à distance sur des ordinateurs ou téléphones.
- Social engineering ; des faux comptes d'organisations demandent aux victimes via les réseaux sociaux de divulguer leurs informations personnelles et financières.

Quelques chiffres clés :

Augmentation des pertes dues à la fraude par rapport à 2019 (par pays) :


27,2%


12,3%


34,6%


41,5%

En France, **59% des personnes** ont été victimes d'au moins un préjudice en ligne, avec les statistiques suivantes :

Fraude en ligne : 12%
Taux de souscription à une assurance contre la fraude : 9%

Les secteurs les plus touchés par **la fraude à l'identité** en ligne sont :
Services financiers - Commerce de détail - Télécommunications

2. Bien identifier les risques

L'ensemble des étapes, qu'elles soient **externes** – vers le client, l'usager ou le prestataire – ou **internes** – entre les différents métiers –, doivent être pensées uniformément, comme une chaîne digitale, pour éviter la rupture ou la « rematérialisation », mais aussi les risques de fraudes. Car le risque apparaît lors de la transmission de fichiers Excel, de la diffusion de mails ou du stockage sur différents serveurs, etc. C'est ici que l'entreprise perd en confiance numérique, car les principales conséquences peuvent être graves : **fraude documentaire, usurpation d'identité, problèmes d'intégrité ou de datation d'un document.** Cela pose aussi la question de la confidentialité. S'il n'y a aucun chiffrement pour les documents transmis simplement par mail, ils peuvent être très facilement modifiés à la volée. Il faut avoir conscience que la cybercriminalité s'est professionnalisée et que les techniques sont de plus en plus sophistiquées.

Alors comment s'y prendre ?

Il faut avant tout identifier où se situent précisément ces risques, afin de mettre en place les bons outils, en repensant la chaîne digitale de manière globale. Pour une entreprise ou une administration, l'une des solutions existantes est de s'appuyer sur un prestataire de confiance. Celui-ci doit disposer de qualifications et de certifications reconnues au niveau **français et européen,** et couvrant tout le scope de **la confiance numérique**. Cela permet avant tout de se poser les bonnes questions à partir d'une vue d'ensemble, d'assurer une réponse complète en termes de sécurité et de garantir le respect des exigences réglementaires.

3. Sécurité et expérience client : trouver le bon équilibre

La cybercriminalité touche désormais tous les secteurs : établissements de santé, administrations publiques, acteurs immobiliers, etc. Et les risques sont désormais présents à toutes les étapes **du parcours client**. On observe aujourd'hui des fraudes au virement dans le cadre des relations quotidiennes entre une banque et son client. D'où la nécessité de sécuriser l'ensemble de la relation d'affaires. **Identitovigilance, conformité, signature électronique, vérification réglementaire…** Tous sont des passages obligés pour garantir une relation client renouvelée. Le tout en intégrant une autre réalité souvent sous-estimée : la persistance, dans un certain nombre de cas, de l'utilisation du format papier et sa coexistence avec le digital.

Mais les véritables enjeux de sécurité sont à envisager au regard d'une autre dimension centrale : **l'expérience client.**

> *« Il s'agit de sécuriser pleinement la fourniture du besoin, tout en proposant le parcours client le plus fluide, avec le moins de ruptures possibles. La clé est de trouver un juste équilibre entre conformité et expérience client, d'autant plus qu'en France les exigences réglementaires sont particulièrement strictes. »*
>
> **Romain Le Formal,**
> Responsable marketing Certigna.

2 La signature électronique : tout savoir, tout comprendre !

1. Accélérer la souscription digitale

Depuis plusieurs années, **la signature électronique** s'est invitée dans les entreprises mais reste souvent cantonnée à un contexte de souscription avec leurs clients. Jusque-là frileuses, elles se sont équipées de solutions de signature en ligne, permettant d'accélérer son usage. Banques et assurances ont été les premières à s'en emparer et se sont interrogées sur le risque attaché à chaque document et processus. L'objectif : accélérer l'onboarding et proposer un parcours digital «sans couture» afin de capter davantage de clients. C'est pourquoi la phase de contractualisation client cristallise de nombreux usages alors que d'autres processus connexes sont tout autant éligibles à la signature électronique. S'appuyer sur une solution globale, mutualisée et capable d'assurer à la fois la vérification d'identité et d'orchestrer la signature électronique devient essentiel dans la démarche.

2. Sécuriser l'acte de signature numérique

Le règlement européen eIDAS, adopté en 2014, a créé un véritable espace numérique commun à l'ensemble de l'Union européenne (UE). L'objectif : **faciliter et sécuriser les opérations entre les États membres.** Pour cela, il définit notamment les exigences liées à la signature et sa valeur légale. La première version du règlement **eIDAS**, toujours en vigueur, dessine ainsi les contours de l'identification électronique, des services de confiance et des documents électroniques. Il définit également les paramètres de **la signature électronique,** et en reconnaît **la valeur juridique.**

Le règlement eIDAS crée notamment trois niveaux de signature électronique :

1 **la signature électronique simple,** facile d'accès et très couramment utilisée, mais dont la valeur sécuritaire reste faible ;

2 **la signature électronique avancée,** qui doit répondre à des exigences plus poussées, notamment en matière de vérification d'identité ;

3 **la signature électronique qualifiée,** qui offre le niveau de sécurité le plus haut.

La très grande majorité des usages peut être couverte par **le 1er niveau** (devis, contrat RH, lettres de mission…). Certaines autres transactions (marchés publics, crédit immobilier) imposent des exigences **légales et réglementaires** propres à chaque secteur d'activité et, de facto, l'usage d'une signature de **niveau avancé ou qualifié.**
Quoi qu'il en soit, l'outil de signature doit offrir toutes les capacités à **couvrir vos usages** et ce, dans l'optique d'être en **conformité**…et en **sécurité.**

A retenir

La signature électronique repose sur des mécanismes de **cryptologie** garantissant l'intégrité d'un acte numérique et l'identification du signataire. Elle nécessite un outil de signature et un certificat attestant de **l'identité du signataire.**

Pour **être reconnue** d'un point de **vue juridique**, la signature électronique doit :

- *être liée au signataire de manière univoque.*
- *permettre d'identifier facilement le signataire.*
- *être activable uniquement par son signataire.*
- *être apposée sur un document ne pouvant être modifié après signature.*

Grâce au procédé sur lequel elle repose, la signature électronique **assure la sécurité des documents.**

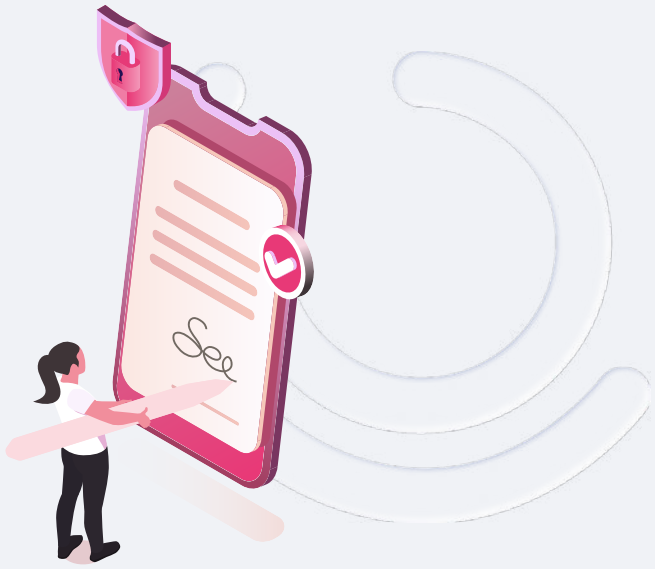
C. Couvrir tous les usages, même en interne

L'outil doit être envisagé dans son ensemble afin de répondre aux besoins de signature tout au long du processus. Prenons un exemple. Même si les risques peuvent varier entre un crédit immobilier, un crédit à la consommation et une ouverture de compte bancaire, il peut exister des étapes sous-jacentes et complémentaires au contrat nécessitant une **signature interne ou externe** *(négociation d'une clause, avenants, clôture d'un compte…)*.
Sans qu'elles soient forcément régies par des exigences réglementaires précises, ces opérations peuvent, elles aussi, être concernées par **la signature électronique** et ce de manière **simple et rapide.**
D'où l'intérêt de choisir un outil capable d'offrir agilité et couverture fonctionnelle riche pour couvrir ces besoins et ainsi éviter la rupture dans la chaîne digitale. Il faut donc dépasser l'acte de souscription pour s'interroger sur ce qui se passe en **amont et en aval.**
Pour accompagner la mutualisation, il convient de s'appuyer sur **une solution globale,** scalable et capable d'assurer à la fois **la vérification d'identité et d'orchestrer les workflows de signature.**

D. Signer : avant tout une expérience utilisateur

La signature électronique n'a rien d'innée pour la grande majorité des personnes. C'est pourtant l'acte le plus important car il scelle un engagement mutuel entre les parties et sa conformité juridique reste le point central de son utilisation. Raison pour laquelle il convient de penser son usage dans un contexte de **parcours et d'expérience client optimale,** afin d'onboarder un maximum de personnes et de fluidifier la démarche. Pour cela, il est important de bien **scénariser le parcours du client** mais aussi **le workflow interne.** C'est-à-dire, définir le circuit que va emprunter le document, les étapes par lesquelles il va passer, déterminer les intervenants (approbateurs, signataires…), les éventuelles délégations, jusqu'à la signature finale de toutes les parties.

Quelles que soient les étapes, il convient de penser à la façon dont l'utilisateur, interne comme externe, va réaliser l'action de manière simple, **fluide et sans rupture.** Car la clé d'une **digitalisation réussie** est bien d'impliquer les collaborateurs qui vont faire usage de l'outil, d'autant plus s'il s'agit d'un moment clé comme **la souscription.** L'interface ne doit donc pas susciter d'interrogations afin d'éviter tout arrêt au cours de la démarche : l'utilisateur doit sentir que c'est simple et intuitif, surtout pour les personnes moins aguerries au digital.



E. Dépasser l'usage de la signature !

Pour relever le défi de **la lutte contre la fraude,** s'appuyer sur un prestataire unique devient **le facteur clé de succès.** Agissant comme un véritable **tiers de confiance,** il est capable de fournir une boîte à outils digitale complète au travers **de solutions technologiques** et services certifiés permettant de sécuriser toutes les étapes du parcours et des processus associés. **Vérification d'identité à distance, authentification de personnes morales ou physiques, horodatage qualifié, signature électronique… Un tiers de confiance** délivre des produits et services qualifiés, dans le respect des exigences européennes et françaises. Sans oublier l'archivage électronique des documents signés qui doivent être conservés de manière probatoire, pérenne et sécurisée.

5 bons conseils pour choisir son outil de signature électronique

1. Impliquer les différents acteurs concernés au sein de l'entreprise

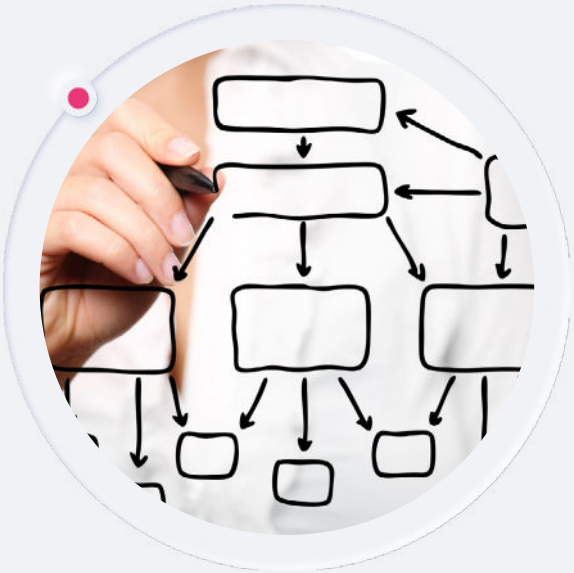
Engager les métiers, les DSI, la direction, et le service juridique dans le choix de signature électronique. Il convient de s'équiper d'un outil de signature capable de **se modeler à l'organisation et les pratiques au sein de l'entreprise.** Tout en gardant **la confidentialité** associée à chaque service/département, unifiez les usages de la signature électronique, rapprochez les services et étendez les fonctionnalités pour plus d'efficacité.

2. Assurer la bonne valeur de la signature électronique

Adapter la solution de signature en fonction du type **de documents, du niveau de sécurité, du signataire, de la dimension légale et de simplicité.** Quelques soient les exigences qui s'imposent à votre secteur d'activité, la solution doit permettre de signer avec les 3 niveaux de signature (simple, avancé et qualifié). A l'issu de l'acte de signature, le document et les preuves de signature sont conservés dans **un système d'archivage électronique,** garantissant leur **intégrité et leur pérennité.**

3. Définir le moyen de déploiement adapté à l'usage

Considérez les facteurs : la volumétrie, l'urgence, les ressources, l'automatisation, pour définir le moyen de déploiement : **plateforme/portail ou API.** Dans le premier cas, l'implémentation de l'outil peut être rapide et nécessiter peu d'accompagnement à condition que les interfaces soient fluides et intuitives. De l'autre, l'API offre davantage d'automatisation et **implique une intégration** au sein de vos outils métiers.



4. Inclure toutes les populations

Pour déployer la signature électronique partout, il faut s'assurer que son utilisation soit **facile et la plus intuitive** possible pour tout un chacun. Car il s'agit de faire signer des personnes qui peuvent coupées du numérique ou pas très aguerries au digital. Le parcours de signature doit donc être **le plus clair possible** afin de n'amener aucune interrogation, amenant à une rupture par l'utilisateur. Une solution respectant **la norme RGAA** peut être une bonne approche.

5. Penser au processus dans son ensemble

La signature électronique du document est certes la finalité mais elle doit s'inscrire dans un processus plus global : collecte de pièces, vérification d'identité, archivage légal… **L'usage de circuits ou workflow** permet d'initier des projets de signature intégrant toutes les phases en amont et en aval. Et bien sûr, de n'oublier personne : l'ensemble des parties prenantes (valideur, signataire, personne à informer…) doit être intégré dans le circuit.

NB : Pensez à l'archivage électronique pour conserver vos documents et dossiers de preuve dans le temps !

Le maillon fort : S'adosser à un tiers de confiance

Les solutions Certigna garantissent **la chaîne de confiance numérique** pour sécuriser chaque étape de **vos parcours clients et processus métiers.**

Conscients que **les enjeux d'échange et de conformité numérique** touchent toutes les activités d'une entreprise, **les solutions Certigna** s'appuient sur **une plateforme unique de services de confiance.** Intégrant différentes briques technologiques, elle garantit **la sécurité, la fiabilité, l'intégrité** ainsi que **la valeur juridique** des transactions et des échanges numériques entre entreprises ou avec des particuliers.

Quel que soit le secteur d'activité, **les solutions Certigna** s'intègrent parfaitement à vos applicatifs en place *(portail client, extranet, intranet salarié, site internet…)* et apportent la méthode adéquate pour répondre aux exigences juridiques qui s'imposent à vous, notamment en matière de **vérification d'identité et de signature électronique.**

En apportant des réponses modulaires ou plus globales, notre plateforme délivre ainsi un catalogue de services technologiques de **confiance à 360°** qui vous aident à :

Identifier : Basée sur le liveness et la biométrie, notre technologie permet d'effectuer une vérification d'identité à distance avec le bon degré de confiance (faible, substantiel et élevé). Ainsi, nous facilitons et sécurisons la démarche d'identification au sein des parcours client au travers d'un processus **100% digitalisé** et sans couture, et ce, jusqu'à la délivrance d'une identité numérique réutilisable.

Authentifier : L'authentification par certificat constitue l'une des solutions techniques de choix pour accompagner les entreprises dans leur transformation digitale. En tant que tiers de confiance, nos certificats numériques permettent de contrôler l'identité d'une personne physique, morale ou d'un serveur avant de lui accorder l'accès ou la communication avec un service.

Signer : En mode portail ou au travers de nos API, vous disposez d'une solution clé en main pour signer et faire signer vos documents avec un niveau simple, avancé ou qualifié suivant vos enjeux de conformité. Grâce aux workflows, vous définissez les étapes d'approbation et de signature et intégrez autant de signataires que nécessaire.

Fiabiliser : En tant qu'Autorité de certification et prestataire de service d'horodatage électronique reconnu au niveau français (Règlement Général de Sécurité) et européen (règlement eIDAS), nous sommes votre partenaire de choix pour garantir la copie fiable et la valeur juridique de vos documents numériques. Qui plus est, afin de lutter contre la fraude documentaire, nous proposons une solution de cachet électronique visible (2D-Doc), véritable dispositif antifraude permettant de renforcer l'identification et l'authentification de vos documents.

Sécuriser : Nos certificats SSL avec validation de l'organisation (OV) garantissent aux visiteurs de votre site que l'Autorité de Certification a vérifié l'existence juridique de votre entreprise. Nos certificats de sécurité SSL RGS remplissent l'ensemble des conditions requises par le Référentiel Général de Sécurité (RGS). Leur présence est un gage de confiance supplémentaire pour les visiteurs qui passent par vos noms de domaine, puisqu'il correspond au niveau d'exigence requis pour les sites de l'administration française.

Garantir : Nos cellules de relation client viennent apporter, lorsque nécessaire, une garantie de conformité ou de traitement supplémentaire pour 100% de vos flux et de vos échanges. Reposant sur l'expertise d'agents spécialisés de middle et de back-office, nous assumons par exemple de bout en bout les exigences d'une vérification d'identité à distance conforme au référentiel PVID. Cette expertise de traitement de la donnée par l'humain est aussi un atout majeur pour assumer un traitement convergent pour les parcours hybrides, mixant différents canaux et types de flux (papier, e-mail, sms, voix...).

CERTIGNA VERIF ID
Hub de vérification d'identité à distance

CERTIGNA SIGN
Solution de signature électronique

CERTIGNA DIGITAL ID
Identité numérique réutilisable

SERVICES DE CONFIANCE
Certificats électroniques, Horodatage qualifié, Cachet électronique visible, SAE

Et après ?

De **la signature électronique à l'identité numérique**

La digitalisation des services est en marche et la crise sanitaire n'a fait qu'accélérer cette tendance : malgré les confinements successifs, nous avons pu continuer à ouvrir des comptes en banque, échanger documents et informations avec les administrations, signer des contrats de travail ou vendre des biens immobiliers.

Simplifier et sécuriser le parcours client ou usager :

Les entreprises et les administrations considèrent désormais **l'identité numérique** comme un objectif majeur. Des réglementations prévoient la généralisation de la **facture électronique** et des mesures de prévention de la fraude, ce qui souligne son importance. Mais la France est en retard dans le déploiement de l'identité numérique par rapport à d'autres pays européens. Il est noté que la France a soumis son schéma d'identité électronique en avril 2021, bien après d'autres pays. Raison pour laquelle les pouvoirs publics ont un rôle à jouer et ont donc un intérêt à soutenir le déploiement de l'identité numérique. Car elle peut **renforcer la compétitivité des entreprises** en simplifiant **le parcours client et en facilitant les ventes à distance.**

Des attentes fortes envers l'eIDAS V2 :

D'abord, concernant le volet identitaire, il faut noter que **l'identité numérique** n'a pas été suffisamment largement déployée dans la première version du **règlement eIDAS**. L'objectif est désormais de diffuser le « wallet », un dispositif qui consistera à regrouper en une application mobile individuelle, à la fois son identité, mais également ses attributs d'identité – permis de conduire, diplômes, attestations de mutuelles, qualifications et certifications de compétences, etc. L'ensemble sera sous la responsabilité personnelle de chaque usager, conservé sur son smartphone et déblocable sous son contrôle uniquement.

L'autre évolution, sur **la confiance numérique,** consistera majoritairement à créer de nouveaux métiers par les effets juridiques qui seront enfin reconnus. En effet, certains services comme **l'archivage électronique** ou encore le **registre électronique (blockchain)** pourront désormais avoir une valeur juridique incontestable.

Du PVID à l'identité numérique :

En 2021, l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** a publié un nouveau référentiel pour les prestataires de **vérification d'identité à distance.** Cela offre un cadre de régulation pour ces prestations, y compris des exigences pour vérifier l'identité à distance.

Mais avec **l'eIDAS V2,** on peut s'attendre, à termes, à ce que le PVID soit progressivement remplacé par des parcours comme le wallet. Toutefois, pour accéder pour la première fois à son wallet, pour son renouvellement – car celui-ci aura une durée de vie limitée – ou pour en obtenir un nouveau suite à une perte, le **PVID** sera certainement le moyen le plus approprié pour vérifier l'identité. Mais pour y arriver, les acteurs de **l'identité numérique** vont devoir faire preuve de pédagogie. Car tout le monde ne dispose pas de la même capacité d'équipement numérique : il faut nécessairement posséder un smartphone, même si **le wallet** sur ordinateur sera aussi potentiellement envisageable.

« Plus que jamais, l'identité numérique s'impose comme un enjeu clé. Cet essor des usages nécessite de garantir l'identification et l'authentification de la personne qui réalise ces opérations. D'autant plus que la multiplication des parcours digitaux se traduit par des centaines de logins et mots de passe, plus ou moins bien gérés. Il s'agit donc de sécuriser l'accès aux services en ligne et de simplifier la gestion quotidienne des dispositifs d'identification. »

Jérôme Bordier,
Directeur associé SEALWeb

Editeur de logiciels innovants, Innovation&trust est la digital factory de Tessi.

Nous développons les solutions numériques qui replacent l'humain au cœur des parcours. Parce qu'ensemble, nous voulons que le quotidien devienne **plus simple, plus sûr et plus responsable,** notre vision repose sur 3 valeurs fondamentales : **Innovation, Cloud Native** et Green IT.

Nous proposons une offre étendue de logiciels en BtoB ou BtoBtoC qui se décline dans 5 domaines : E-Santé (Wizcare), Confiance numérique (Certigna), Gestion de contenus et processus métiers (Sqalia), CRM et processus client (OnCustomer), Devops & Services Cloud.

Servant 2 000 clients et 1,5 million d'utilisateurs, Innovation&trust compte 250 collaborateurs dédiés à la Tech au sein de 3 centres de Recherche & Développement en France, en Espagne et au Maroc. Innovation&trust fédère également un écosystème ouvert de plus de 80 acteurs innovants, grâce à Pépites Shaker, son programme européen accélérateur de startups.

Conscients que la transition digitale des organisations est loin d'être aboutie, les équipes Innovations&trust ont à cœur d'accompagner les entreprises et administrations dans leurs projets de transformation au travers de solutions technologiques adaptées aux usages et pratiques des équipes.

Innovation&trust
Human interactive first

Immeuble ileo
27-33 Quai Alphonse le Gallo
92100 Boulogne-Billancourt
www.tessi.eu