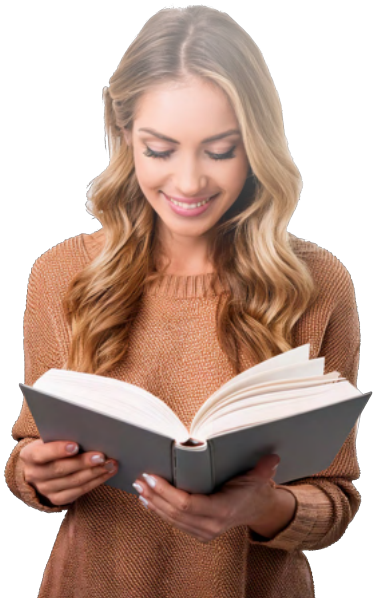
beys

WALLET & CONFIANCE NUMÉRIQUE

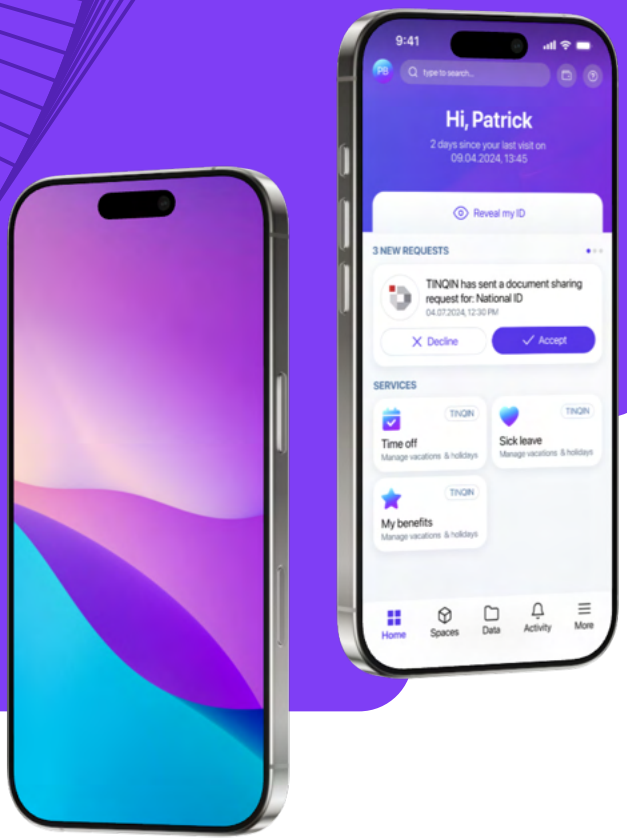
Maîtrisez La Nouvelle Réglementation Européenne eIDAS 2

Table des **matières**



21
eIDAS 2 : VOS NOUVEAUX DÉFIS

23
RELEVEZ LES DÉFIS INTRODUITS PAR eIDAS 2 ET ALLEZ BIEN AU-DELÀ AVEC BEYS



Qu'est-ce que le règlement eIDAS ?

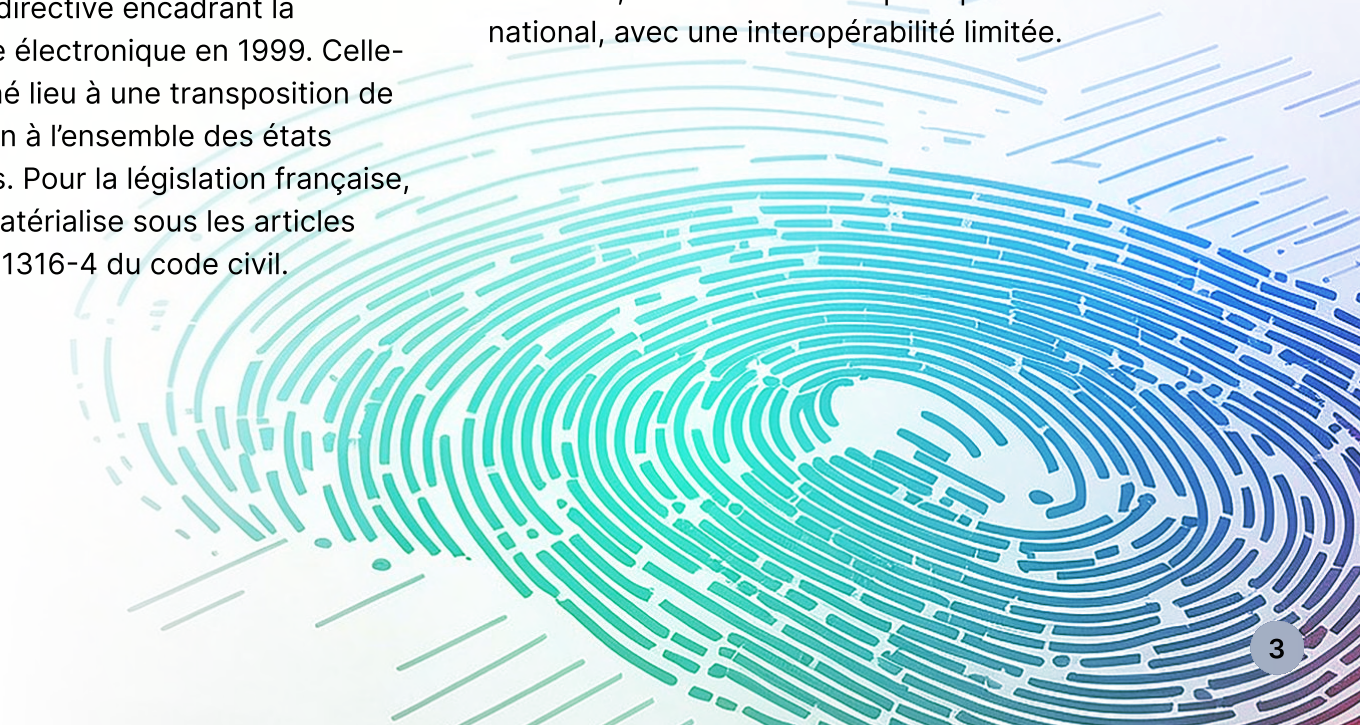
Electronic Identification, Authentication and Trust Services

PREMIÈRE INTERVENTION EUROPÉENNE : UN PEU D'HISTOIRE

Avec l'apparition de nouveaux usages digitaux et le développement des échanges numériques à la fin des années 90, il est apparu essentiel d'instaurer un cadre réglementaire pour sécuriser les échanges, particulièrement les engagements pris. C'est dans ce contexte que l'Union européenne adopte pour la première fois une directive encadrant la signature électronique en 1999. Celle-ci a donné lieu à une transposition de législation à l'ensemble des états membres. Pour la législation française, elle se matérialise sous les articles 1316-1 à 1316-4 du code civil.

Cette première étape est cruciale car elle a établit la force probante de l'écrit électronique, désormais équivalente à celle de l'écrit papier, ainsi que la signature électronique et les exigences de fiabilité, conformément au décret n° 2001-272 du 30 mars 2001.

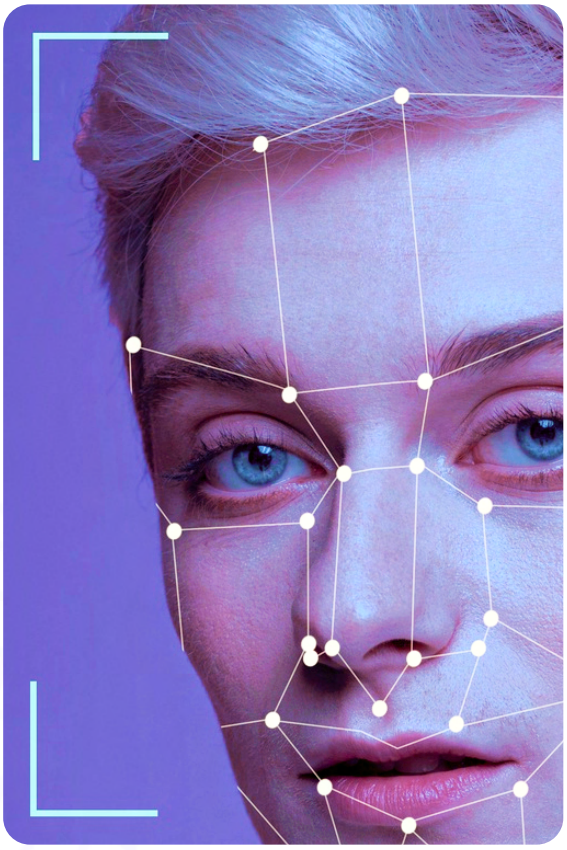
La directive européenne marque alors, en ce début des années 2000, la prise en compte des échanges digitaux et pose les premières fondations de leur cadre juridique. Cependant, cette incursion réglementaire reste timide, ne prévoyant la signature électronique que dans le champ des services de confiance numérique, sur lesquels nous reviendrons dans ce livre blanc. En raison de la diversité des transpositions dans les états membres, cet outil est resté principalement national, avec une interopérabilité limitée.



LE RÈGLEMENT eIDAS DE 2014

Le règlement eIDAS vise à dépasser les limites des premières initiatives du législateur européen dans le domaine des services de confiance numérique. Pour ce faire, trois niveaux d'action ont été définis :

- La définition de « l'identité numérique » devant être diffusée par chaque état membre auprès de ses citoyens.
- L'introduction de nouveaux services de confiance.
- L'instauration d'un cadre européen unifié de surveillance des prestataires de confiance numérique.

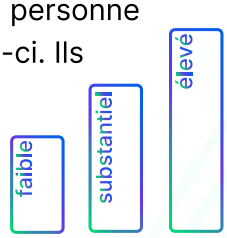


L'IDENTITÉ NUMÉRIQUE TELLE QU'INTRODUITE PAR LA COMMISSION EUROPÉENNE

Le règlement eIDAS impose aux états membres la mise en œuvre de schémas d'identification électronique.
Ces schémas sont définis comme étant un système d'identification électronique, attribuant des moyens d'identification aux personnes physiques ou morales, ou à leurs représentants.

Qu'est-ce qu'un moyen d'identification électronique (MIE) ? Un MIE est défini comme « un élément matériel et / ou immatériel contenant des données d'identification personnelles et utilisé pour s'authentifier sur un service en ligne ». Les citoyens européens peuvent ainsi s'identifier facilement en fournissant une preuve de leur identité auprès d'acteurs publics ou privés en ligne.

La preuve de cette identité est assortie de trois niveaux de fiabilité : faible, substantiel et élevé. Ces niveaux sont définis par des critères d'identification de la personne et d'authentification de celle-ci. Ils sont utilisés en fonction du risque lié au service et au cadre réglementaire entourant celui-ci.



Les moyens d'identification électronique peuvent être délivrés :

- Par l'État membre ;
- Dans le cadre d'un mandat de l'État membre ;
- Indépendamment de l'État membre, mais devant être reconnu par celui-ci ;

PANORAMA DES SERVICES DE CONFIANCE DÉFINIS PAR eIDAS

Le règlement inclut un service de validation pour garantir la validité des signatures électroniques et un service de préservation pour assurer leur intégrité dans le temps.

La signature électronique :

Le règlement eIDAS définit la signature électronique (simple, avancée et qualifiée) ainsi que le cachet électronique, permettant aux organisations de garantir l'émission d'un document.

L'horodatage :

L'horodatage, quant à lui, permet d'assurer la date des transactions.

Les certificats électroniques :

Les certificats électroniques de signature sont également prévus pour les sites web avec les certificats d'authentification de site web. Ainsi, l'organisation peut non seulement garantir l'identité des personnes physiques et morales mais aussi celle des services.

L'envoi recommandé :

L'envoi recommandé électronique représente une garantie de délivrance d'un document électronique. Ce dernier sera repris en droit français dans la définition de la lettre recommandée électronique.

Autres services :

Le règlement inclut un service de validation pour garantir la validité des signatures électroniques et un service de préservation pour assurer leur intégrité dans le temps.

UN CADRE EUROPÉEN UNIFIÉ DE SURVEILLANCE DES PRESTATAIRES DE CONFIANCE NUMÉRIQUE

eIDAS
Qualified Trust
Service Provider

Il existe une distinction non négligeable entre services de confiance numérique et services de confiance numérique qualifiés : les premiers sont délivrés par des prestataires de confiance, les seconds, eux, sont délivrés par des prestataires de confiance qualifiés.

Les prestataires de services de confiance qualifiés sont soumis à des audits réguliers et portent une responsabilité quant aux services délivrés. La compétence du prestataire de services de confiance, et a fortiori du prestataire de services de confiance qualifié, intervient à plusieurs niveaux :

- Technique : déployer et maintenir des solutions fiables.
- Juridique : garantir la valeur probante et maitriser le risque associé au service. Les prestataires de services de confiance qualifiés sont soumis à une obligation de résultat.
- Financier : prévoir les fonds nécessaires au maintien de l'activité y compris dans le cadre d'une cessation d'activité.
- Organisationnel : prévoir et déployer les procédures de contrôle nécessaires pour garantir le niveau de service attendu.
- Sécuritaire : anticiper les risques, prévoir les mécanismes de surveillance et notifier l'organe de contrôle de tout incident de sécurité.

Il appartient à chaque État membre de définir un organe de supervision pour surveiller les activités de prestataires de services de confiance et de maintenir à jour les listes européennes des services de confiance qualifiés (l'ANSSI en France, l'ILNAS au Luxembourg, le BSI en Allemagne, etc.)

Une partie de la confiance introduite dans le règlement eIDAS repose sur cet encadrement et cette responsabilité des prestataires de services de confiance.

Le règlement eIDAS 2 : Pourquoi introduire une **nouvelle version ?**

Le monde digital évolue rapidement et l'adoption des nouveaux services reste incertaine à ce jour. Le législateur a donc pris soin de fixer une clause de révision, prévue dans l'article 49 :

> *La Commission procède à un réexamen de l'application du présent règlement et rend compte au Parlement européen et au Conseil, au plus tard le 1er juillet 2020.*

En cela, le règlement eIDAS est un véritable outil d'accompagnement juridique des pratiques de confiance numérique.

Il s'adapte au gré de l'évolution des capacités et des usages et renforce le cadre d'application.

LES NOUVEAUX SERVICES DE CONFIANCE

De nouveaux services de confiance sont alors ajoutés au sein du règlement. Les principaux services couverts par eIDAS 2 sont :

La gestion de dispositifs de création de signature électronique à distance

Cette prestation permet de distinguer l'émission de certificat de signature de son utilisation. Lorsque l'on parle de signature électronique, les deux notions sont régulièrement associées.

- L'émission du certificat de signature correspond à la vérification de l'identité et la délivrance des moyens permettant de signer. Ces moyens peuvent être délivrés sur un support physique, une carte à puce par exemple, ou sur un serveur à distance.

- L'opération de signature électronique consiste à utiliser ces moyens de signature.

Lorsqu'il s'agit d'un support physique, aucun prestataire n'est utile. En revanche, lorsque le moyen de signature est hébergé à distance il doit être géré par un prestataire de service. Ce prestataire gère la création de signatures électroniques à distance.

L'archivage électronique

L'archivage est défini comme

> *Un service assurant la réception, le stockage, la récupération et la suppression de données électroniques et de documents électroniques afin d'en garantir la durabilité et la lisibilité, ainsi que d'en préserver l'intégrité, la confidentialité et la preuve de l'origine pendant toute la période de préservation.*

Ce service était jusqu'à présent régi essentiellement par des normes nationales. Le règlement eIDAS 2 permet de venir l'unifier dans les différents états membres et de renforcer ainsi son interopérabilité.

Le registre électronique

Le registre électronique est un ajout important de cette deuxième version d'eIDAS. Le législateur le définit tel que :

> *une séquence d'enregistrements de données électroniques qui garantit l'intégrité de ces enregistrements et l'exactitude du classement chronologique de ces enregistrements.*

Il s'agit d'une avancée notable. Ce registre électronique est caractérisé comme une preuve d'intégrité et de chronologie.

La délivrance d'attestation d'attribut électronique.

Qu'est-ce qu'une attestation d'attribut électronique ? Il s'agit d'un document qui certifie un ou plusieurs attributs d'identité. Cette attestation peut par la suite être transmise par la personne physique ou morale, dont elle émane au tiers de son choix. Ce dernier est probablement, celui qui se distingue le plus. Il permet à des prestataires de service de confiance de délivrer des attestations sur un ou plusieurs attributs d'une personne. Un attribut est défini comme

> *Une caractéristique, une qualité, un droit ou une autorisation d'une personne physique ou morale ou d'un objet.*

Ces attestations ont la même force probante qu'une attestation papier. Il est donc dorénavant possible d'attester de la qualité d'une personne ou d'une information partielle sur son identité par voie électronique.

Ces attestations sont centrales dans l'usage du portefeuille européen d'identité numérique (le Wallet).

Les différentes facettes de l'identité :

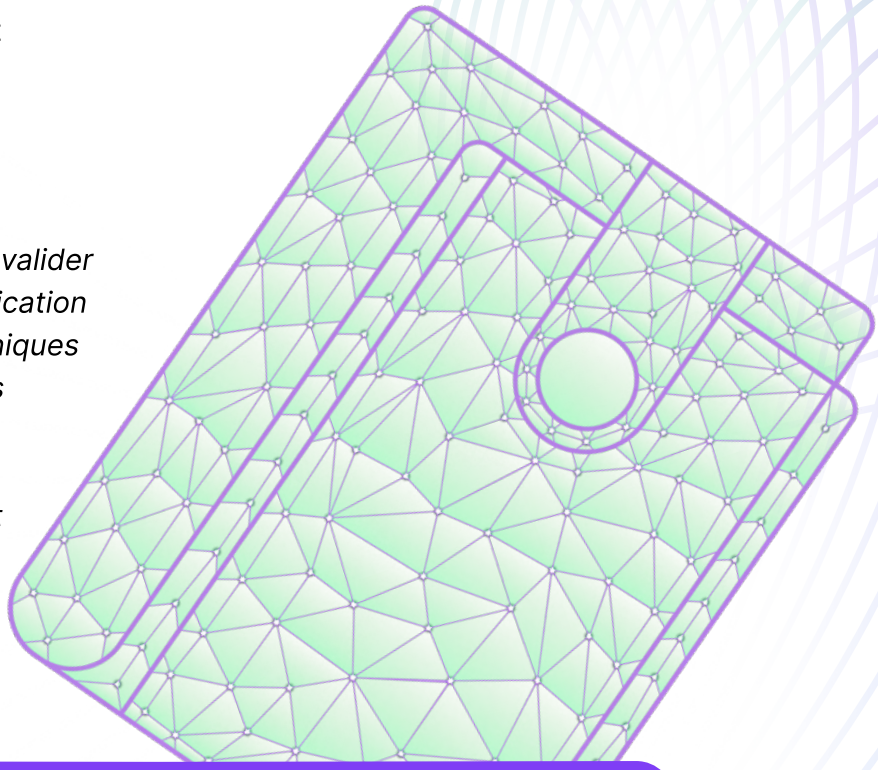
On peut différencier une identité « régalienne », liée à l'état civil d'une personne et utilisée dans des démarches administratives ou officielles, d'une identité « non régalienne ». Cette dernière peut correspondre à un pseudonyme, par exemple sur un site de rencontres, ou à un nom et prénom d'usage (reconnus ou non par l'État), utilisés pour des achats en ligne.

LE WALLET EUROPÉEN D'IDENTITÉ : PIERRE ANGULAIRE D'eIDAS 2 DE QUOI S'AGIT-IL EXACTEMENT ?

Le wallet européen est l'évolution naturelle de l'identité numérique introduite dans la première version d'eIDAS. Dans cette ancienne version, nous parlions de moyen d'identification électronique délivré selon un schéma d'identification notifié par un état membre.

Dans la deuxième version du règlement eIDAS, le wallet est défini comme :

> *un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique. Le wallet permet également de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés*



Cachet électronique vs signature électronique.

Le cachet électronique est l'équivalent numérique du tampon d'entreprise. Il permet aux entreprises et aux entités publiques de sceller des documents, garantissant ainsi l'authenticité de l'émetteur, l'intégrité du contenu et la lisibilité des documents transmis par voie électronique.

La signature électronique s'adresse quant à elle aux personnes physiques. Elle nécessite une action directe de la part du signataire, qui doit vérifier le document à signer. Cela implique donc un engagement du signataire sur le contenu du document.

De façon plus synthétique, il s'agit d'une application mobile sécurisée permettant de gérer l'identité d'une personne physique ou morale et ses relations avec des parties utilisatrices.

Il va bien au-delà du moyen d'identification, car il permet en particulier :

1. De demander, stocker, gérer et transmettre à des parties utilisatrices des attestations attributs et des données personnelles d'identification.

2. De générer des pseudonymes et de les stocker localement sous forme chiffrée dans le portefeuille européen d'identité numérique.

3. D'authentifier en toute sécurité le portefeuille européen d'identité numérique d'une autre personne et de recevoir et partager des données d'identification personnelle et des attestations électroniques d'attributs de manière sécurisée entre les deux portefeuilles européens d'identité numérique.

4. D'accéder à un journal de toutes les transactions effectuées avec le portefeuille européen d'identité numérique, au moyen d'un tableau de bord commun qui permet à l'utilisateur :

    a. De consulter une liste à jour des parties utilisatrices avec lesquelles l'utilisateur a établi une connexion et, le cas échéant, de toutes les données échangées ;

    b. De demander facilement l'effacement par une partie utilisatrice de données à caractère personnel en vertu de l'article 17 du règlement (UE) 2016/679 ;

    c. De signaler facilement une partie utilisatrice à l'autorité nationale chargée de la protection des données compétente, lorsqu'une demande de données présumée illégale ou suspecte est reçue.

5. De signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés.

6. De télécharger, dans la mesure où cela est techniquement possible, les données de l'utilisateur, l'attestation électronique d'attributs.

7. D'exercer les droits de l'utilisateur à la portabilité des données.

Au-delà de la simple définition et du catalogue des fonctionnalités, il est essentiel de se projeter dans son utilisation ainsi que dans l'adhésion des citoyens européens. En effet, comme pour les moyens d'identification électronique, les Etats ont l'obligation de proposer aux utilisateurs un wallet d'identité numérique. Toutefois, les utilisateurs ne sont pas tenus d'en posséder un.

Pour étudier différents cas d'usage, la Commission européenne a mis en œuvre des pilotes à grande échelle organisés par différents consortiums.

Focus sur les consortiums dans le cadre d'eIDAS 2

Un consortium regroupe différentes organisations publiques et privées. il s'est créé en réponse à l'appel à projets lancé par la Commission européenne dans le cadre du programme "pour une Europe numérique". Ce programme vise à promouvoir l'utilisation des technologies numériques par les administrations publiques, les citoyens et les entreprises.
A ce jour, quatre consortiums ont été créés pour réaliser des pilotes sur l'identité numérique européenne.
Le 1er consortium teste le wallet dans six cas d'usage : services publics électroniques, ouverture de comptes bancaires, enregistrement de carte SIM, permis de conduire électronique, signature électronique qualifiée à distance et prescription médicale électronique.
Le 2ème consortium s'est quant à lui positionné sur un projet pilote de paiements transfrontaliers.
Le 3ème consortium s'attache à développer un projet pilote axé sur l'utilisation du wallet dans le contexte des voyages.
Enfin, le 4ème consortium travaille sur les cas d'usage liés aux diplômes, aux qualifications professionnelles et à la sécurité sociale.

Conjointement, des travaux d'architecture ont été initiés pour définir des formats et standards d'implémentation. Sans cela, l'interopérabilité nécessaire aux wallets des différents pays ne sera pas possible.

Comme pour les moyens d'identification électroniques, les wallets devront être délivrés de trois façons :

- Directement par un État membre ;
- Sur mandat d'un État membre ;
- Indépendamment d'un État membre tout en étant reconnus par cet État membre.

Il n'existera donc pas un wallet européen mais des wallets européens (a minima un par État membre) avec des fonctionnalités pouvant être ajoutées. La liste de parties utilisatrices et des prestataires d'attestation d'attributs pourra également varier selon les wallets.

Domaine public

domaine privé

Ce wallet servira non seulement à l'utilisation des services publics mais aussi pour des usages dans le secteur privé. Les services d'identification et de confiance inhérents à ce wallet faciliteront grandement la vie des individus et des entreprises : prouver son identité avec un fort degré de fiabilité, contractualiser, stocker des données... Tout cela en redonnant à chaque partie prenante la souveraineté sur ses données.

Que signifie exercer sa souveraineté sur ses données ?

Être souverain signifie avant tout avoir le contrôle. Lorsque l'on parle de souveraineté sur les données, il s'agit de définir qui a le contrôle et la capacité à agir sur celles-ci et quels sont les fondements de ce contrôle. Cette notion est étroitement liée à la protection des données, à leur gouvernance et à leur cycle de vie. Exercer sa souveraineté sur ses données c'est en reprendre le contrôle, pouvoir décider à qui, quand, pour combien de temps et pour quels usages les données sont partagées, avoir une information exacte quant à leur utilisation, leur stockage et ce qui est mis en œuvre pour les protéger.

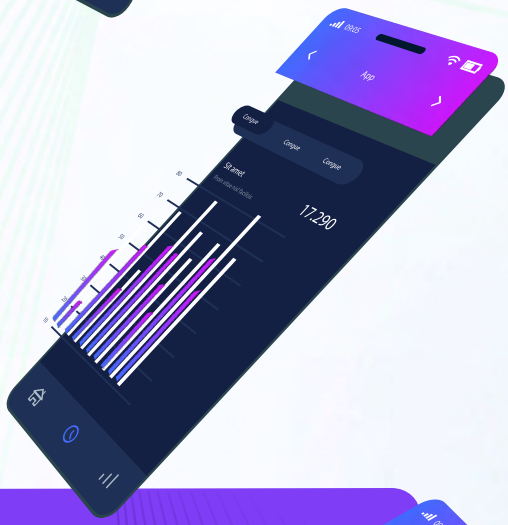
QUELLES SONT LES LIMITES DU WALLET EUROPÉEN ?

Le wallet européen tel qu'il est défini dans le règlement est un minimum attendu.

Mais ce minimum est-il suffisant ?

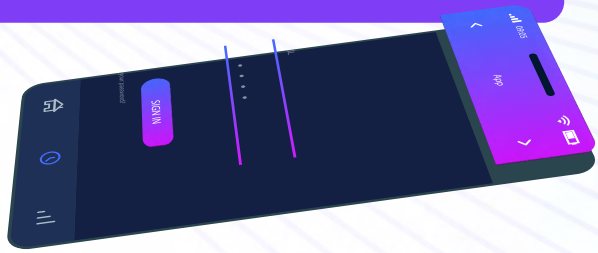
La multiplicité des fournisseurs d'attributs

L'Architecture and Reference Framework (ARF) rappelle bien que l'utilisateur du wallet doit s'assurer en premier lieu que le wallet fournit les services et est connecté avec les fournisseurs d'attestation d'attributs et les fournisseurs de service qui lui sont nécessaires.



Quelle est la mission de l'ARF ?

L'ARF propose un cadre structuré pour la conception d'un wallet d'identité numérique. Il précise les technologies et composants requis, tels que des protocoles de communication standardisés, des interfaces utilisateurs intuitives et des mécanismes de sécurité solides. L'objectif est de garantir une expérience utilisateur fluide tout en assurant un haut niveau de sécurité. Ce cadre veille également à ce que le wallet réponde aux attentes de tous les utilisateurs, tout en protégeant les données personnelles conformément au RGPD.



La première limitation peut donc venir de la richesse des fournisseurs d'attributs accessibles au travers du wallet. Ces attestations seront l'élément central du wallet car elles permettront de définir l'identité des utilisateurs tout en ne donnant accès qu'aux données strictement nécessaires pour l'usage prévu par la partie utilisatrice.

Le transfert d’informations

Le wallet est une application mobile. Or, il n’est pas prévu d’opération de sauvegarde et de transfert d’information en cas d’utilisation de plusieurs équipements, cependant cette fonctionnalité n’est pas interdite. Pour la mettre en œuvre, il faudra nécessairement prévoir un stockage extrêmement sécurisé, totalement inaccessible au prestataire de wallet.

Ce même stockage est une force pour conserver tout autre information en dehors des attestations d’attribut et données d’identité prévues au règlement.

Le partage de documents sécurisé est alors possible avec une traçabilité particulièrement complète et sûre.

La nécessité de prévoir des services supplémentaires

Selon les cas d'usage, des services supplémentaires pourront être nécessaires à l'utilisateur pour interagir avec un tiers. Ces services ne devront toutefois pas être fournis directement par ce dernier. Par exemple, comment gérer en tant qu’utilisateur ma vie de salarié vis-à-vis de mes employeurs, ma vie de locataire vis-à-vis de mes bailleurs, … Ces services devront être ajoutés en complément du wallet lui-même.

Ainsi, eIDAS 2 ne prévoit pas de service de lettre recommandée électronique intégré au Wallet. Le législateur a cependant choisi d’inciter les fournisseurs de service d’envoi recommandé à être opérables avec le Wallet et se réserve le droit de fixer les conditions d’interopérabilité via un acte d’exécution.

Synthèse des avancées entre les deux versions du **règlement eIDAS**

Caractéristiques / Version	eIDAS 1.0	eIDAS 2.0
Champ d'application du règlement	Réglemente les signatures électroniques, les transactions électroniques, les organismes concernés et leurs processus d'intégration afin d'offrir aux utilisateurs un moyen sûr de faire des affaires en ligne.	Élargit le champ pour inclure des services numériques transfrontaliers supplémentaires, tels que l'authentification et l'identification avec le wallet d'identité numérique.
Sécurité et vie privée	Définit un niveau élevé de sécurité et de respect de la vie privée.	Renforce la sécurité et la confidentialité des identités électroniques et des services de confiance.
Identité numérique	Ne fournit pas de cadre pour la création et l'utilisation d'identités numériques.	Établit un cadre pour la création et l'utilisation d'identités numériques, connues sous le nom de "portefeuille d'identité" ou wallet européen.
Interopérabilité	N'a pas mis l'accent sur l'interopérabilité entre les systèmes nationaux.	Améliore l'interopérabilité entre les systèmes nationaux.
Services de confiance qualifiés	N'inclut pas les services d'archivage électronique, les grands livres électroniques, la gestion des dispositifs de création de signatures et de sceaux électroniques à distance, ou l'attestation électronique qualifiée d'attributs vérifiés par rapport à des sources authentiques.	Ajoute quatre nouveaux services de confiance qualifiés : services d'archivage électronique, grands livres électroniques, gestion de dispositifs de création de signatures et de sceaux électroniques à distance et attestation électronique qualifiée d'attributs vérifiés par rapport à des sources authentiques.
Conformité avec le RGPD	Non applicable.	Conforme au règlement général sur la protection des données (RGPD).

Synthèse des avancées entre les deux versions du **règlement eIDAS**

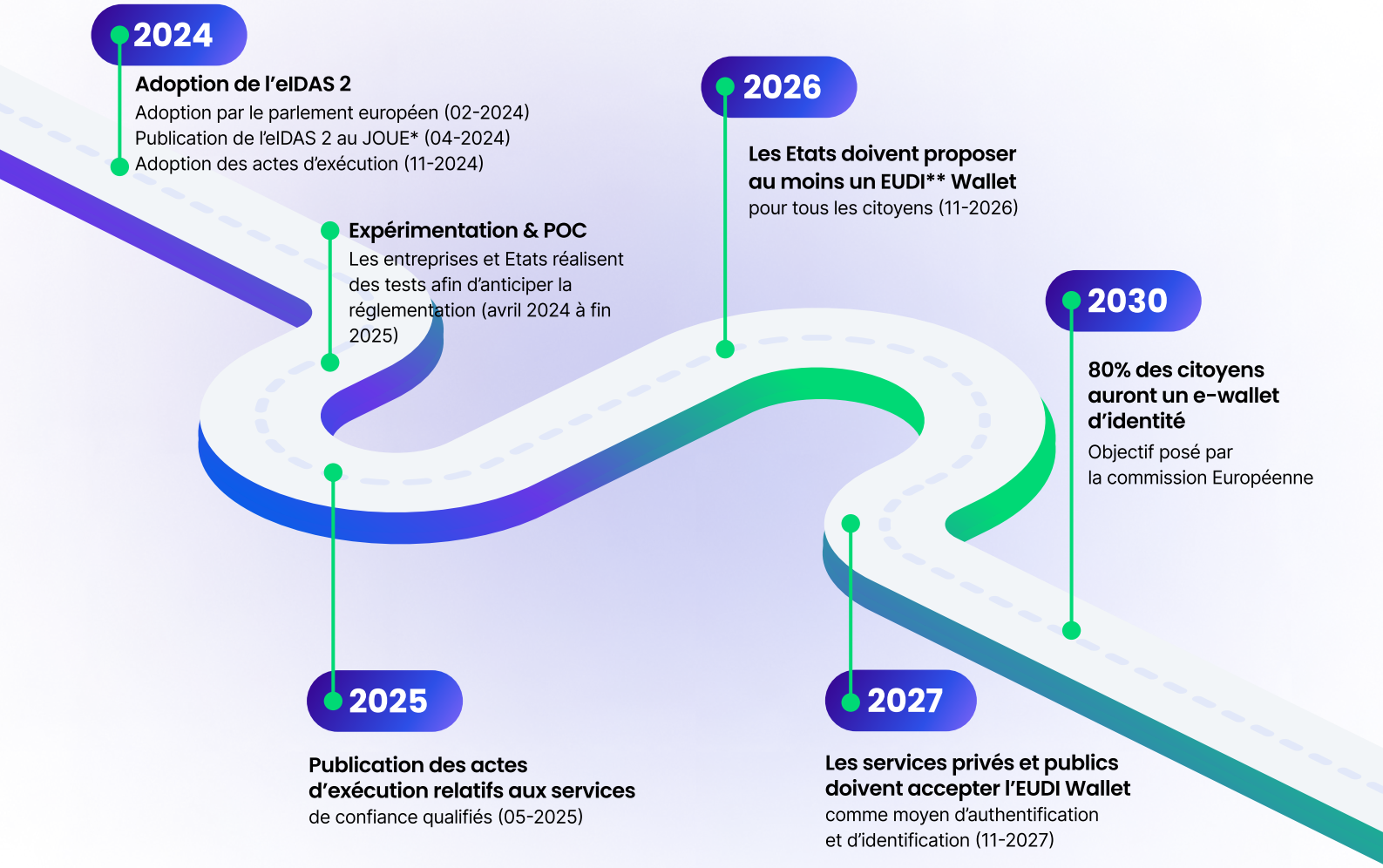
Caractéristiques / Version	eIDAS 1.0	eIDAS 2.0
Wallet d'identité numérique (EU Digital Identity Wallet)	Non applicable.	Définit un portefeuille numérique sécurisé devant être accessible tant aux citoyens qu'aux entreprises et organisations de l'Union européenne. Ce portefeuille sert principalement comme un moyen d'identification électronique (MIE) avec un niveau élevé de garantie, permettant l'émission, le stockage et la vérification d'attestations électroniques d'attributs d'identité. L'objectif global est de faciliter et sécuriser les échanges de données en offrant la possibilité de présenter des attestations numériques.
Contrôle de l'utilisateur	Critiqué pour sa trop grande rigidité et le fait qu'il ne permette pas aux utilisateurs de contrôler totalement leurs informations d'identification.	L'accent a été mis sur le "contrôle exclusif", permettant à tous les citoyens de l'UE d'exercer leurs droits à une identité numérique qui reste entièrement sous leur contrôle.

Les actes d'exécution et les **prochaines étapes**

Le règlement établit un cadre général, qui peut être précisé par des actes d'exécution.

Ces actes pourraient en partie répondre aux limitations du wallet mentionnées précédemment. A la différence de la première version du règlement, la commission doit les publier, pour la plupart, selon un calendrier défini :

- 21 novembre 2024 pour les actes relatifs au Wallet ;
- 21 mai 2025 pour les actes relatifs aux services.



*JOUE = Journal officiel de l'Union européenne **EUDI = European Union Digital Identity

Qu'est-ce qu'un acte d'exécution ?

Un acte d'exécution est un acte non législatif qui définit des règles détaillées permettant la mise en œuvre uniforme d'actes juridiquement contraignants de l'Union Européenne.

eIDAS 2 : **Vos nouveaux défis**

Que change eIDAS 2 pour vous ?

L'organisation et l'interaction dans les relations commerciales et la vie des entreprises s'apprêtent à prendre un autre sens. Alors qu'aujourd'hui les services de signature, et plus généralement, les services de confiance, sont mis en place par des entreprises pour le compte de leurs utilisateurs. La refonte du règlement eIDAS sépare clairement les rôles pour tendre vers une identité auto-souveraine.

Ainsi, le workflow de contractualisation utilisé dans tout système de souscription n'aura plus la charge de la vérification de l'identité du souscripteur. Celle-ci sera obtenue au travers du wallet de ce dernier. De même l'opération de signature ne sera plus gérée exclusivement par le service de contractualisation mais en partie par le wallet et le prestataire de gestion de signature qualifiée.

Il en est de même sur les dispositifs de connaissance client mise en œuvre par les secteurs réglementés (KYC). A ce jour, les entreprises soumises à cette règlementation réalisent ou font réaliser sous leur responsabilité les vérifications nécessaires. Grâce au wallet, tout ou partie de ces vérifications pourront être déléguées à des prestataires d'attestation électronique d'attribut transmises directement par le client via son wallet.

Pourquoi est-ce important **pour votre entreprise ?**

La porte ouverte par l'Union européenne au travers du wallet et les services de confiance associés peut permettre aux entreprises de s'inscrire dans des usages éminemment novateurs. A condition de savoir identifier un partenaire parfaitement conforme et hautement fiable, les entreprises trouveront des espaces de valeurs significatifs dans leur façon d'adresser de multiples sujets :

- Améliorer l'efficience du KYC (Know Your Customer) en favorisant l'ergonomie, en réduisant les coûts et en maîtrisant les risques.

- Gagner en efficience grâce à la signature électronique qualifiée intégrée, permettant une rationalisation des processus d'engagement et d'acceptation et la mise en place de procédures commerciales innovantes.

- Renforcer la confiance des clients en maîtrisant l'identité des acteurs, la qualité des données, la pertinence des traitements et ainsi s'affirmer sur le marché.

- Augmenter la solidité de la signature avec un usage généralisé à tous et pour tous les services.

- Réduire les coûts et les temps de traitement inhérents à l'échange de documents tout en assurant leur véracité.

Le règlement eIDAS 2 constitue une opportunité unique d'accéder à un vivier d'usages et de clients nouveaux. Explorons les enjeux et challenges à relever pour transformer les outils apportés par eIDAS 2 en atouts pour votre entreprise.

Relevez les défis introduits par eIDAS 2 **et allez bien au-delà avec BeYs**

A condition de vous appuyer sur un partenaire spécialiste, reconnu tiers de confiance qualifié pour exploiter pleinement le wallet, vous aurez une opportunité unique de vous différencier sur le marché tout en adressant les enjeux de votre entreprise :

CONFORMITE

La maîtrise des risques numériques demeure la clé de voûte dans le choix de votre suite de services de confiance. Il est nécessaire d'assurer votre conformité sur toute la chaîne de vos processus. L'enjeu est de taille au vu de la complexité réglementaire et de son évolution régulière. La maîtrise du risque juridique et des risques financiers encourus en cas de défaillance de votre part vous demande une forte vigilance dans le choix de vos partenaires, ainsi que de posséder une vision à 360° de tous les paramètres.

CONFIANCE

Une transformation constante des technologies du numérique, des usages sans cesse renouvelés… il s'agit non seulement de continuer à s'inscrire dans ces évolutions mais également de préserver la confiance qui vous lie à vos clients. Gérer les risques d'usurpation d'identité et de falsification des documents, tout en garantissant la sécurité des données qui vous sont confiées constitue le socle de la confiance qui vous sera accordée.

EXPERIENCE CLIENT

Une expérience client réussie passe par un parcours client fluide et efficace. Simplifier le parcours client assure un meilleur taux de conversion et une satisfaction accrue tout au long de la vie des services. Il faut également veiller à renforcer la connaissance des utilisateurs et la qualité des services, en disposant de données à jour. De cette façon, vous fidélisez vos clients et gagnez en productivité.

GAIN DE PRODUCTIVITE

Accroître son efficience économique et préserver sa compétitivité sont deux axes clés dans la bonne marche de vos activités. Pour cela, il est important de bâtir une stratégie vous permettant de vous concentrer sur votre cœur de métier et d'externaliser les fonctions supports auprès d'un partenaire de confiance. Ainsi, vous disposez des expertises nécessaires et réduisez vos coûts. Une stratégie partenariale efficace vous permet de digitaliser efficacement vos parcours clients et gagner significativement en productivité.

DIFFERENCIATION

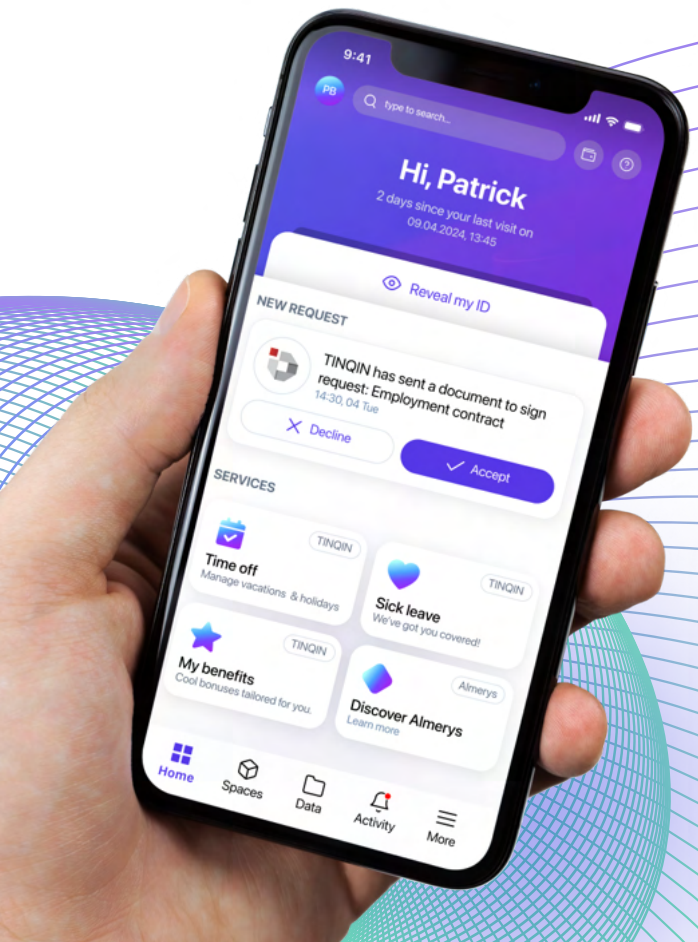
Dans un marché en expansion, faites la différence ! Une fois vos risques juridiques, liés à la conformité, maitrisés, il vous reste à définir une stratégie différenciante pour valoriser vos services. En offrant à vos clients des services et des offres personnalisés, dans un environnement numérique ultra-sécurisé, vous créez les bases d'une meilleure connaissance client, d'échanges enrichis et développez votre chaîne de valeur.

BeYS : Un tiers de confiance certifié, **expert et indépendant**

SE METTRE AU SERVICE DE CHAQUE PARTIE PRENANTE…

BeYs bénéficie de 25 ans d'expertise dans le traitement industriel et la gestion des données sensibles. Dès les années 2000, le groupe BeYs apparaît comme un acteur disruptif dans la gestion des données sensibles. La vision fondatrice du groupe est d'agir pour le compte et l'intérêt des individus tout en étant au service de ses partenaires en proposant des traitements de données sécurisés juridiquement, faisant de BeYs un tiers de confiance expérimenté et certifié.

La marque de fabrique du groupe est de développer by design toutes les briques nécessaires à la chaîne de confiance numérique. Le développement de services de confiance numérique adossé à une maîtrise pointue des risques juridiques associés positionne BeYs comme votre partenaire de confiance, fiable, expert et au service de vos intérêts. La modularité et l'interopérabilité des services développés par BeYs résultent de l'engagement fort du groupe au service de ses partenaires pour leur fournir un service toujours plus performant et entièrement dédié à leurs besoins, à la souveraineté sur le patrimoine de données numériques et à leur efficience économique. Fort de ses 25 ans aux côtés de partenaires de tous secteurs (banques, mutuelles, professions réglementées, grandes entreprises, institutions), BeYs offre aujourd'hui un service précurseur, ultra sécurisé et cyber résilient en créant un écosystème numérique de confiance porteur de valeur pour toutes les parties prenantes.



… ET PARTAGER UNE VISION UNIQUE GRÂCE À KIPMI®, LE WALLET AUGMENTÉ BY BeYs

Kipmi®, le wallet européen augmenté qui va au-delà **de la norme eIDAS 2**

	EU wallet eIDAS 2	Wallet Kipmi
Unifier les données dans un espace dédié	✓	✓
Les conserver en toute sécurité	✓	✓
Partager seulement les données nécessaires	✓	✓
Contractualiser en intégrant la signature qualifiée	✓	✓
Conserver l'historique des données, en tracer le partage, en révoquer l'accès	✓	✓
Gérer tous types d'identité (pro, perso,..) avec enrichissement continu	•	✓
Proposer un espace dédié aux prestataires de services	•	✓
Intégrer différents fournisseurs d'ID pour une couverture complète	•	✓
Disposer de workflows intégrés et sécurisés via des API	•	✓
Bénéficier de fonctions avancées de nomination / délégation de signature	•	✓

Bien plus qu'un simple portefeuille d'identité numérique, Kipmi® révolutionne votre façon de gérer votre patrimoine de données numériques, vos interactions numériques personnelles ou professionnelles, et vos relations avec vos prestataires de services.

Découvrez comment cette plateforme innovante, conforme aux dernières réglementations européennes, peut simplifier votre vie numérique et renforcer votre confiance dans l'écosystème digital.

Une sécurité à l'épreuve **du temps**

BÉNÉFICES POUR VOS CLIENTS

- Simplifier ses démarches en ligne grâce à son identité numérique
- Sécuriser ses transactions et se protéger contre l'usurpation d'identité
- Maîtriser ses données : savoir qui les utilise, quand et pourquoi
- Gérer et valoriser son patrimoine digital
- Exercer pleinement ses droits RGPD
- Mettre à jour et/ou révoquer à tout moment le partage de ses données personnelles
- Obtenir des services personnalisés

BÉNÉFICES POUR VOTRE ENTREPRISE

- Bénéficiez de données utilisateurs actualisées et qualifiées
- Accédez à tous types d'identités (personnes physiques, morales, objets)
- Assurez votre conformité réglementaire (RGPD, eIDAS, AML/LCB-FT, NIS2...)
- Profitez d'un accès exclusif dans la galerie des prestataires pour proposer vos services
- Automatisez en toute sécurité l'accès à vos offres avec des données à jour

Kipmi® au cœur de votre **transformation digitale**

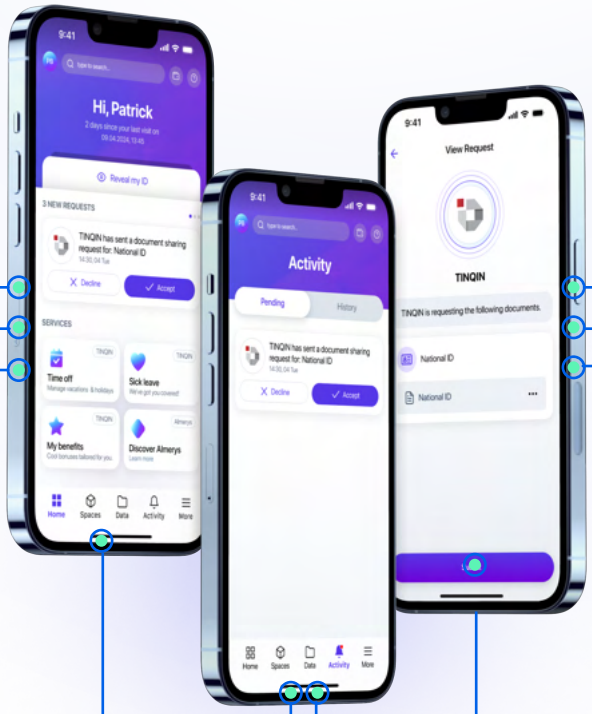
Kipmi ® est en effet bien plus qu'une simple solution d'identification numérique. C'est un véritable catalyseur de transformation digitale, conçu pour répondre aux défis spécifiques de nombreux secteurs d'activité

VOICI UN APERÇU DES MULTIPLES FACETTES DE NOTRE SOLUTION :

Signature qualifiée pour une présomption de fiabilité et accélérer en toute confiance vos transactions.

Certification d'une identité pour chaque utilisateur conforme aux exigences légales et aux réglementations.

Ecosystème : Kipmi® peut être utilisé dans un contexte personnel aussi bien que professionnel et dans de nombreux secteurs d'activité pour disposer d'un écosystème de services personnalisés.



Création d'une identité numérique conservée et utilisée de manière sécurisée dans Kipmi® grâce au chiffrement de bout en bout.

Véritable console de pilotage des droits des personnes grâce à une conformité RGPD by design pour assurer le plein contrôle des données personnelles.

Galerie de services pour offrir à des collaborateurs, des clients et partenaires, un espace professionnel au sein de Kipmi® et mettre en avant vos outils et vos services. L'application mobile devient aussi un canal de communication sécurisé.

Moyen d'Authentification forte délivré pour faciliter votre conformité à la directive NIS2.

Nomination – délégation pour permettre de faire le lien entre personne physique et personne morale, de gérer les rôles, responsabilités et délégations pour ainsi tracer les engagements pris.

KYC « Know Your Customer » pour vérifier en votre nom l'identité de vos clients conformément aux exigences légales et aux réglementations.

Lettre recommandée électronique pour simplifier et accélérer vos communications.

Grâce à son architecture modulaire et interopérable, Kipmi® s'intègre de manière transparente à votre écosystème digital, vous permettant de tirer rapidement parti de la puissance de l'identité numérique pour transformer votre activité.

Focus sur nos premiers **cas d'usage**

EMPLOYEE LIFE

Alliez innovation technologique et expertise humaine pour optimiser votre stratégie RH et distinguer votre marque employeur.

1
Accélérez et sécurisez les process de recrutements

2
Gérez et pilotez les droits RGPD pour protéger les données des collaborateurs

3
Facilitez l'accès à toute une gamme de services et avantages

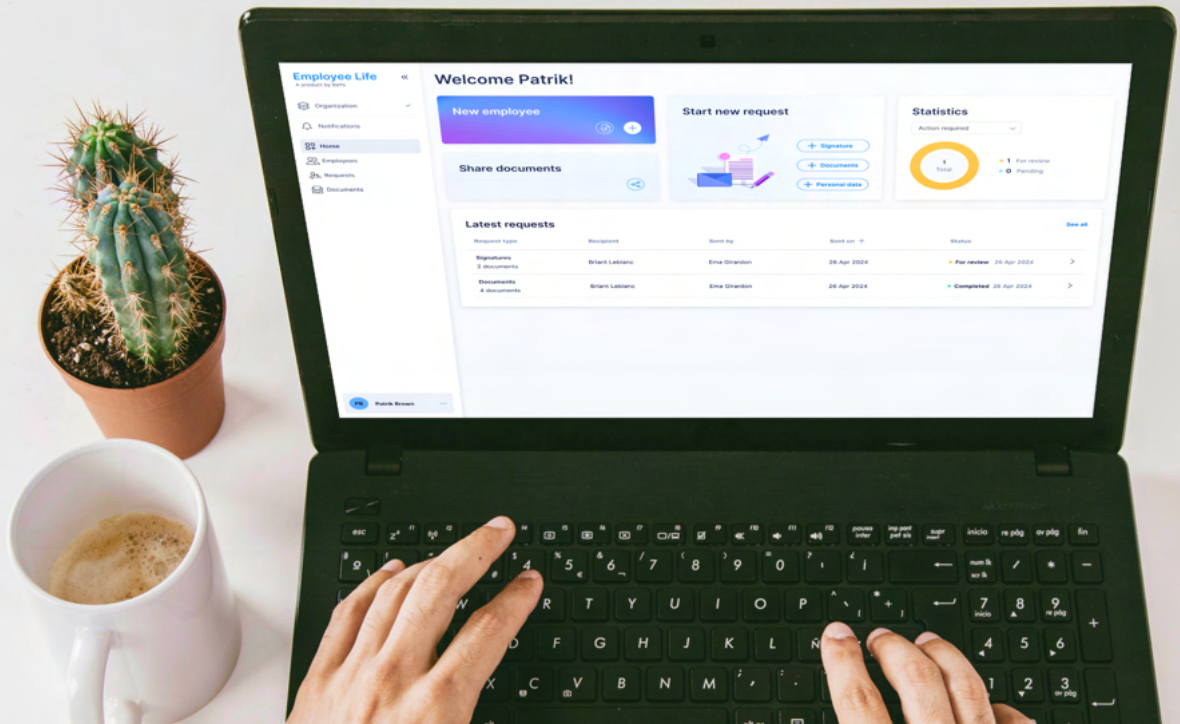
4
Garantissez votre conformité réglementaire, en vous appuyant sur un tiers de confiance certifié

5
Bénéficiez d'une personnalisation sans limite pour ajouter facilement une multitude de services pour les collaborateurs

6
Assurez une gestion fine des accès et habilitations (bâtiments, logiciels...) pour assurer le secret des affaires

7
Simplifiez la transmission des documents administratifs

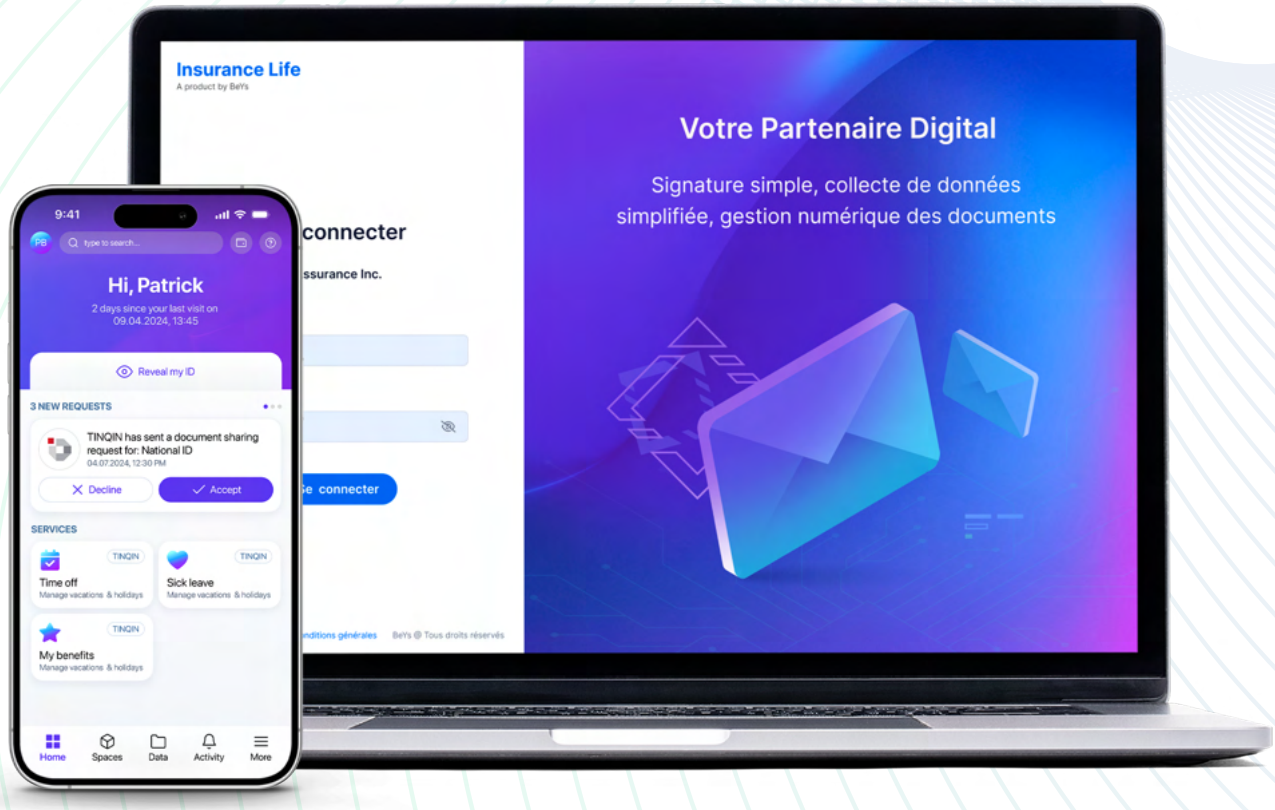
8
Alignez votre stratégie RH avec tous les sites de l'entreprise



Focus sur nos premiers **cas d'usage**

INSURANCE LIFE

Votre partenaire de confiance au service de votre performance assurantielle



1

Appuyez-vous sur des données personnalisées et des modèles prédictifs pour offrir des conseils et services sur mesure, visant à améliorer le bien-être des assurés et réduire l'absentéisme

2

Sécurisez l'accès aux données sensibles des assurés

3

Anticipez les besoins des assurés grâce à l'analyse prédictive

4

Luttez efficacement contre la fraude documentaire

5

Proposez des services innovants pour vous démarquer sur le marché

6

Garantissez votre conformité réglementaire en vous appuyant sur un tiers de confiance certifié

7

Optimisez les coûts de traitement grâce à l'automatisation intelligente

beys

BeYs, expert reconnu en solutions d'identité et de confiance numérique, est un prestataire de services de confiance certifié. Grâce à sa plateforme Trust360, BeYs propose une gamme complète de services, incluant la vérification d'identité, les avis recommandés électroniques, le coffre-fort numérique, et bien plus, tous conformes aux réglementations européennes.
BeYs s'engage pour accompagner chaque citoyen dans la protection de son patrimoine de données en lançant Kipmi®, un wallet augmenté qui va bien au-delà de la réglementation eIDAS 2.

BeYs dispose également de ses propres centres d'hébergement basés en France, Luxembourg et Suisse pour assurer une parfaite maîtrise de son patrimoine de données.
Nos solutions sont adaptées à tous les secteurs et respectent la confidentialité des utilisateurs finaux.

www.be-ys.com