Signature électronique dans les Paiements

FPF/FnTC

1 Introduction

La FnTC et FPF ont décidé d'approfondir en commun la question de la sécurisation et de la prévention de fraude des paiements scripturaux, en particulier les paiements irrévocables et/ou temps réel.

La **Fédération des Tiers de Confiance du Numérique**[1] est une association qui regroupe des fournisseurs de services prenant une part active dans la définition, la mise en œuvre et la promotion de la confiance dans l'économie numérique.
France Payments Forum[2] est une association de professionnels européens, essentiellement français, de services financiers.
Ces 2 organisations ont associé leur expertise pour analyser la pertinence de l'utilisation de services de confiance pour sécuriser l'identité des acteurs « payeur » et « payé » et la validation du paiement. L'objet de cette analyse se limite à exposer ce qu'apporterait la signature électronique à des processus de paiement en complément des mécanismes déjà en place.
Cette démarche résulte du constat que même si une transaction de paiement est sécurisée, une identité du payeur ou du payé frauduleuse (usurpée ou fausse) peut constituer une faille de sécurité, qui ne sera pas forcément détectée lors du consentement lié à la transaction.

Les services de confiance ont pour objectifs notamment de garantir l'authenticité d'une identité, d'un acte et de la préservation de l'acte. De fait, ces services couvrent en particulier l'**identification**, **l'authentification**, la confidentialité, l'intégrité, et la non-répudiation, notamment par le recours à une **signature électronique,** en garantissant des niveaux de confiance. Le présent document analyse l'Identité et la Signature numériques qui sont les deux piliers de la chaine de confiance pour une transaction électronique sécurisée. L'archivage à vocation probatoire pourra être utilisé pour conserver les preuves liées à la signature et pour préserver la chaine de confiance.

L'existence de réglementations européennes sur le paiement et les services de confiance permettent de s'appuyer sur des principes, des règles et des certifications organisationnelles et techniques qui sont reconnues en **France et en Europe**.

Le Règlement européen **eIDAS** : **E**lectronic **ID**entification, **A**uthentication and trust **S**ervices) porte sur les **services de confiance et l'identité numérique et va connaitre une révision, dénommée eIDAS2.**

Le Règlement eIDAS a pour but d'apporter une **harmonisation juridique européenne** sur les services de confiance en définissant des niveaux de **garantie** liés aux niveaux de **l'identification et l'authentification**.

- ✓ **Contrôles et vérifications** effectués durant l'**enrôlement** ou la transaction
- ✓ L'authentification, avec l'**authentification forte** mais aussi en définissant des niveaux de **fiabilité** des **signatures électroniques** qui peuvent partiellement dépendre du niveau de garantie de l'identité utilisée
- ✓ de la **sécurité** utilisée pour déclencher la signature

[1] www.fntc-numerique.com/
[2] www.francepaymentsforum.eu/fr/home/

En parallèle, les réglementations et échanges bancaires se sont renforcés sur la sécurité des transactions, de l'identité des payeurs et des payés, entre autres :

- ✓ La **DSP2**, directive européenne a renforcé la prévention avec l'authentification forte lors des paiements à distance.
- ✓ L'**AMLD**, les dernières versions de la directive sur la lutte anti-blanchiment d'argent. L'ACPR, avec sa transposition dans le Code Monétaire et Financier, a permis d'encadrer l'enrôlement, en particulier à distance, en s'appuyant sur la réglementation eIDAS.

Dans un ordre d'idée plus technique, l'**EBICS** (Electronic Banking Internet Communication Standard) est un protocole sécurisé pour les transactions bancaires en ligne en Europe. Il intègre de l'authentification forte et des signatures électroniques pour l'identification des acteurs.

On note donc que les **réglementations bancaires et eIDAS** pour la signature intègrent la **vérification de l'identité** de tout ou partie des acteurs d'une transaction et la sécurisation des échanges pour limiter la fraude. Lorsque l'identification ne porte que sur une partie des acteurs, certains fraudeurs utilisent cette faille d'identification (« faux fournisseur », « faux commerçant »…).

En l'état actuel des paiements, l'exigence d'un renforcement majeur de la sécurité des transactions de paiement ne semble pas prioritaire. Mais, plusieurs éléments conduisent à réfléchir au futur, notamment le développement de nouveaux instruments de paiement, le virement instantané, et à terme, l'euro numérique, mais aussi les développements technologiques en matière de puissance des algorithmes ou des ordinateurs...

La Commission Européenne veut tout à la fois accélérer le déploiement du virement instantané, irrévocable et temps réel, et le lier avec les Wallets d'identité numérique européens, pour anticiper les fraudes qui vont augmenter avec les flux.

La FnTC et FPF se sont fixés pour but d'analyser les besoins et usages, et d'évoquer l'opportunité et les pistes de solutions avec signature électronique qui pourraient s'intégrer dans les usages actuels et également futurs, avec ou sans l'EWID, le futur portefeuille européen d'identité numérique (eID).

2 Signer un paiement, quel avantage ?

Une signature de personne physique concrétise le consentement à un acte, une action, que ce soit le texte d'un document, une fiche d'intervention, un bon de livraison ou un processus comme le paiement électronique, le tout avec une vocation probatoire.

La définition « réglementaire » d'une signature électronique est la suivante :

- ✓ « *une signature électronique est constituée de données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer » (Règlement* eIDAS article 3.10) :

  et

- ✓ *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.* (Article 1367 al. 2 du Code Civil)

La fiabilité de la signature et de son faisceau de preuve, en cas de litige ou de fraude, est primordiale.

La signature électronique est un mécanisme qui doit permettre de prouver un consentement en s'appuyant sur des processus sécuritaires pour fournir une **garantie de fiabilité** sur :

- ✓ **l'authenticité** de l'origine : identité du signataire
- ✓ **l'intégrité** : le document ne doit pas pouvoir être modifié dans le temps.

⇒ **Avec la signature électronique, signature et éléments signés doivent être liés.**

La qualité et la fiabilité de l'identité et de la signature permettent de mieux lutter contre la fraude.

Toute signature électronique est potentiellement **recevable**, sa fiabilité repose :

- ✓ Sur le niveau de signature et de certificat utilisé
- ✓ Sur le faisceau de preuves associé

Et peut s'appuyer sur des niveaux de signature plus ou moins élevés en fonction :

- ✓ De l'analyse juridique du risque portée par l'acte
- ✓ Du cadre réglementaire sous-jacent

⇒ **Une signature électronique implique donc une vérification de l'identité du signataire, plus ou moins exigeante en fonction du niveau retenu de la signature. En conséquence, une signature électronique fiable offrira une véritable assurance de vérification de l'identité du signataire.** La fraude sur les paiements électroniques scripturaux

Ce chapitre repose sur l'excellent rapport 2021 de l'Observatoire de la Sécurité des Moyens de Paiement (OSMP). Ci-après une cartographie des paiements en volume de transactions.

.

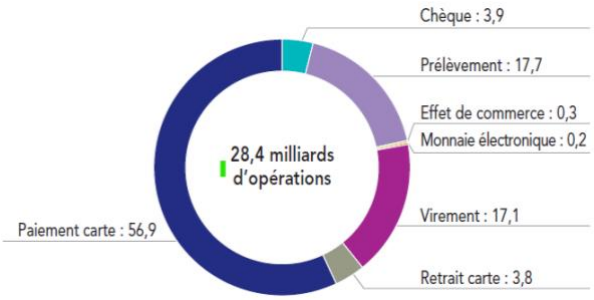


Figure 1 - Source OSMP - Usage des moyens de paiements scripturaux en %

Le podium en nombre de transactions est le suivant :

1. Paiement carte : 56,9%
2. Prélèvement : 17,7%
3. Virement : 17,1%

La carte bancaire reste le moyen de paiement scriptural le plus utilisé en nombre de transactions, et continue à progresser en volume de transactions : plus de 2 % de hausse entre 2020 et 2021.

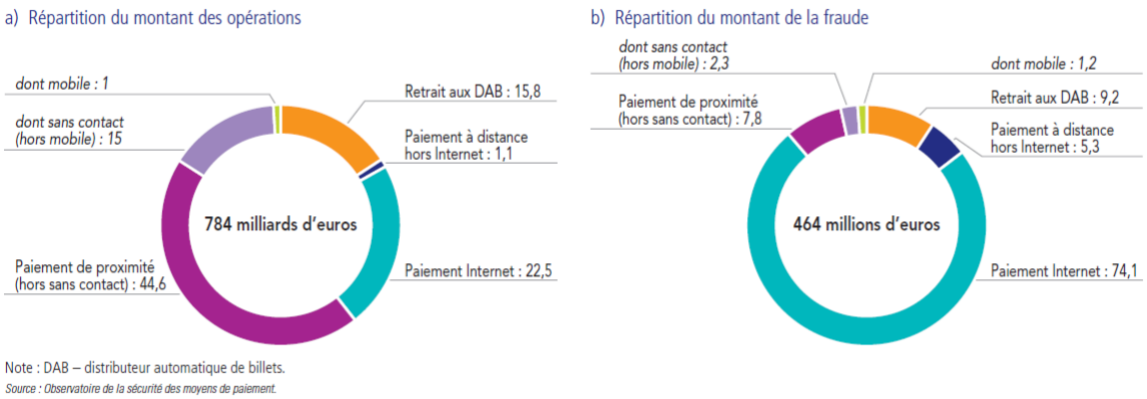
L'usage du chèque continue de diminuer, la fraude ayant amené le commerce et certaines professions à ne plus accepter ce moyen de paiement. L'essentiel de la fraude sur le chèque est porté par la fraude à l'identité (fausse ou usurpée). Les autres moyens de paiement dématérialisés prennent le relais.

En 2021 la fraude porte principalement sur les paiements à distance, les paiements temps réel et/ou irrévocables, dans l'ordre :

1. Le paiement carte à distance
2. Le paiement sans contact par mobile
3. Le virement instantané

4 Le paiement carte sans contact

Le canal d'utilisation des cartes émises en France en 2021 (en %)

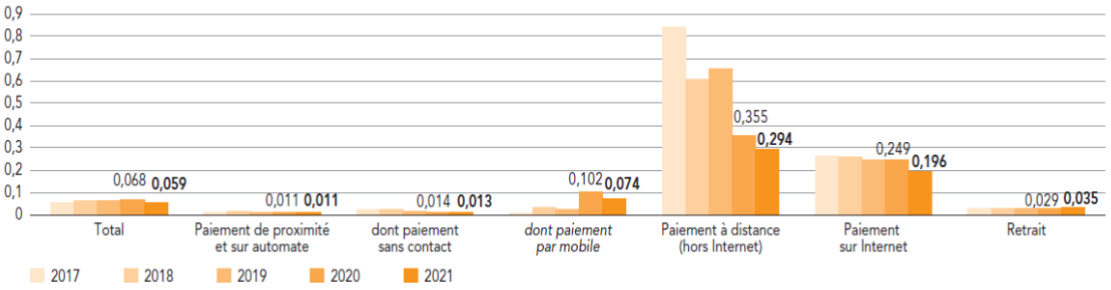


Note : DAB – distributeur automatique de billets.

Source : Observatoire de la sécurité des moyens de paiement.

Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2021 § 1.2.1

G11 Évolution des taux de fraude en montant sur les cartes françaises par canal d'initiation (en %)



Source : Observatoire de la sécurité des moyens de paiement.

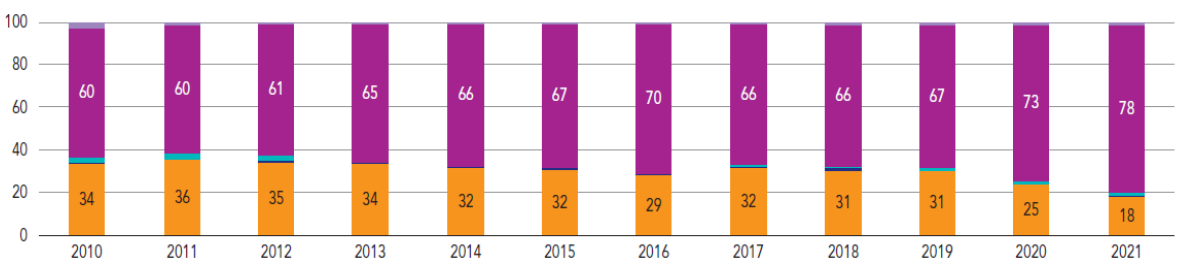
Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2021 § 1.2.1

Pour **les transactions par carte**, le recours à l'authentification forte avec la DSP2 a permis une chute notable du montant total de la fraude sur les cartes françaises : moins 1,9% en 2021.

Les paiements sans contact représentent un très faible montant de fraude, quasiment identique à celui des paiements de proximité traditionnels. La fraude sur ces paiements est à son niveau historique le plus bas, tandis que son usage augmente fortement, tout en restant modeste.

Dans le tableau ci-dessous on peut remarquer que **la part des numéros de carte usurpés** augmente d'année en année en particulier par hameçonnage, tandis que la fraude liée à la perte ou le vol diminue (grâce en particulier à l'authentification forte).

G16 Évolution des typologies dans les montants de fraude depuis 2010 (en %)



Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2021 § 1.2.3

Pour finir pour **le paiement par carte à distance**, bien qu'il ne représente que 20% du nombre de transactions nationales, il représente 70% de la fraude en montant.

Le virement classique est le troisième moyen de paiement le plus fraudé mais reste particulièrement faible et maitrisé.

Le virement instantané est en pleine progression : en 2021 le nombre de transactions a plus que doublé. Il représentait en 2021 2% des virements (flux). Ce type de paiement est voué à progresser, avec l'utilisation du mobile et son faible coût. Sa sécurité pour le moment est assurée en émission. Le taux de fraude est en hausse et très proche des paiements par carte.
Les fraudes à l'identité du payeur et du payé cohabite.

L'OSMP note enfin une hausse de la fraude au **prélèvement,** et le **chèque** reste une source importante de fraude.

Conclusion partielle

Le **point commun** entre les fraudes au virement, fraude au chèque ou prélèvement, c'est qu'elles sont issues souvent de **fraudes à l'identité**.

Les fraudes portant l'identité du payeur ou du payé augmentent et cette année l'OSMP consacre le chapitre 3 de son rapport à « **l'Identité Numérique et la sécurité des paiements** ». En effet, la fraude avec l'usurpation et la fausse identité du payeur ou du payé va augmenter parce que les flux dématérialisés augmentent.

Et, l'OSMP a noté que **même si la sécurité des paiements a augmenté, la fraude à l'identité permet de contourner cette sécurité** et donc ce type de fraude risque d'augmenter :

- ✓ en amont : usurpation d'identité au moment de l'entrée en relation (onboarding)
- ✓ durant le paiement
  - usurpation de l'identité du payeur, via un site marchand avec carte préenregistrée, autorisation de prélèvement, usurpation des coordonnées d'un tiers
  - usurpation de l'identité du payé (via un faux site marchand, particuliers à particuliers, fraudes au « Président », « fournisseur », « notaire », et non-conformité entre identité du payé et IBAN présenté)

Il note que le développement de la dématérialisation des relations administratives et commerciales crée de nouvelles possibilités de fraude, en particulier la fraude à l'identité.

Le chapitre consacré à l'identité du rapport de l'OSMP, détaille l'usage des identités européennes numériques, régaliennes ou non et fait un focus sur l'exemple Suédois.

En effet, la Suède dispose depuis 2003 d'un système d'identité numérique basé sur l'identité et l'identification bancaire (BankID). Cette identité est utilisée pour les services publics et privés, mais également pour signer des paiements et relève des services de confiance au sens eIDAS. **La Suède est une société cashless et relève malgré tout de faibles taux de fraude mais note la montée de certaines fraudes (faux destinataire en particulier de transferts temps réel)**[3].

3 eIDAS

3.1 Signature eIDAS

Aux termes du règlement (eIDAS - art. 25-3) « **l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite** » et, en application du décret 2017-1416 du 28 septembre 2017, une signature électronique qualifiée eIDAS entraîne présomption de fiabilité du procédé d'identification garantissant le lien avec l'acte auquel la signature s'attache. Une signature électronique qualifiée eIDAS entraîne donc renversement de la charge de la preuve car, si pour les

[3] Cf. https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report-2022/

signatures électroniques simples ou avancées, la partie s'en prévalant est tenue de prouver l'identité du signataire et le lien avec l'acte signé, pour les signatures électroniques qualifiées, c'est à la partie contestant la signature de prouver que celle-ci n'a pas valablement identifié son signataire ou que l'acte signé a été altéré. Cette différence de traitement a bien sûr des conséquences importantes et positionne la signature électronique qualifiée comme instrument privilégié de sécurisation des interactions numériques. Bien évidemment, le Juge reste seul maître pour déterminer si la signature électronique qualifiée permet le renversement de la charge de la preuve comme l'énonce expressément l'article 288-1 du Code de Procédure Civile.

Cela étant, « *l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée*. » (eIDAS, art. 25-1)

Toutes les autres signatures électroniques sont recevables devant un juge dès le moment où la preuve de leur fiabilité est rapportée.

Pour les signatures simples et avancée, le cas échéant, des moyens complémentaires peuvent être apportés comme preuve supplémentaires.

L'ANSSI précise les conditions entourant 4 niveaux de signature découlant de la lecture du Règlement eIDAS :

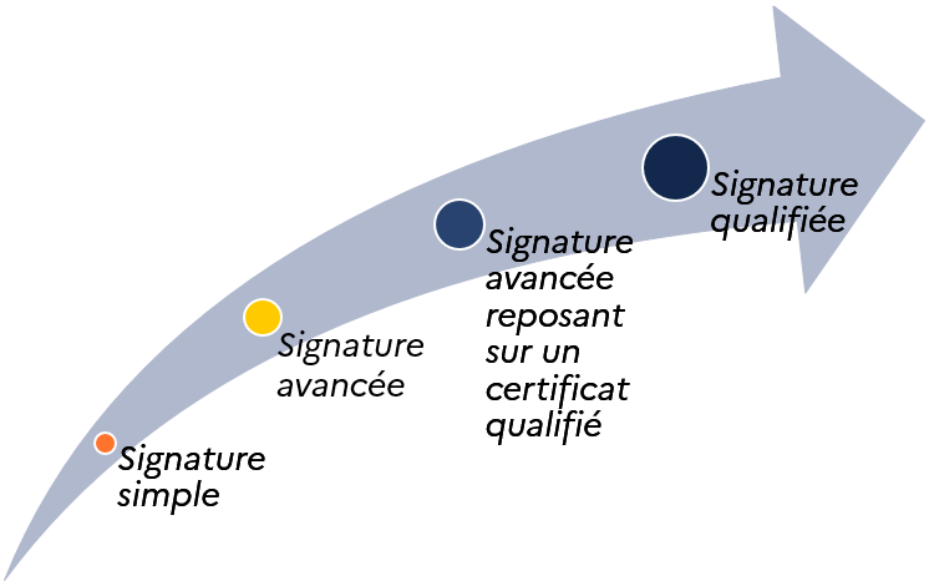


Figure 2 -source ANSSI eIDAS définit 4 niveaux de signature

La complexité de mise en œuvre et la friction sur le parcours augmentant en même temps que la valeur légale se renforce, il s'agit de trouver un équilibre satisfaisant…

Chaque pays européen a chargé son organisme de contrôle de cadrer l'application du règlement eIDAS. En France, il s'agit de l'ANSSI. La matrice ci-dessous extraite du « Guide de sélection du niveau des signatures et des cachets électroniques » publié par l'ANSSI intègre les notions d'interopérabilité entre pays européen en particulier.

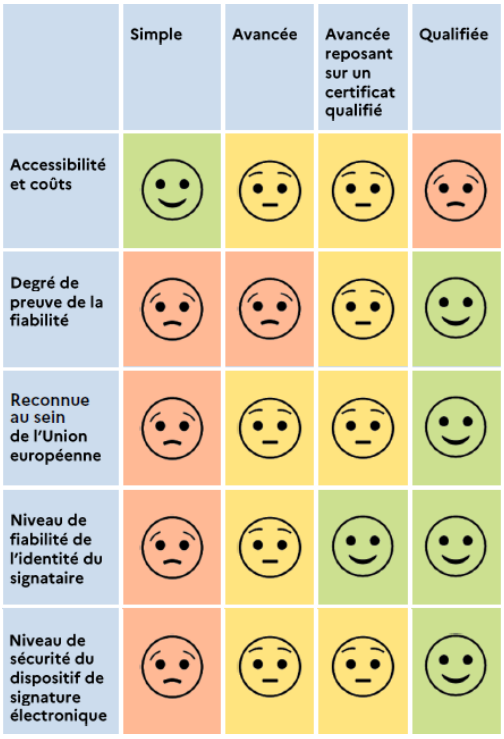


Figure 3 – source ANSSI – Caractéristiques Signature eIDAS

La signature qualifiée est la seule signature permettant une interopérabilité européenne garantie et une présomption de fiabilité. Cependant la signature qualifiée est coûteuse à mettre en œuvre et nécessite un dispositif qualifié pour le signataire en France.

Tandis que la valeur des signatures simples et avancées repose sur la **fiabilité du faisceau de preuves** qui accompagne la signature.

3.1.1 Niveaux de garantie des Identités numériques

Le règlement eIDAS définit **3 Niveaux de garantie pour les identités numériques** afin d'instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres – reconnaissance obligatoire pour les Etats européens depuis 2018 et en France courant 2023*, si le pays a notifié une identité numérique :

- ✓ **Faible** : à ce niveau, l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- ✓ **Substantiel** : à ce niveau, l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- ✓ **Élevé** : à ce niveau, l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Les 2 derniers niveaux permettent l'émission de certificats électroniques qualifiés en application des règles eIDAS actuelles (On notera toutefois que le projet de règlement eIDAS 2 propose de limiter cette possibilité aux seules identités numériques de niveau élevé – voir projet d'article 24).

3.1.2 Niveaux de fiabilité de la Signature

Pour la signature électronique, le Règlement eiDAS V1 prévoit trois niveaux de fiabilité et définit les procédés techniques pour deux d'entre eux (Avancé et Qualifié) :

- ✓ La signature électronique **simple**, englobe tout type de solution correspondant à « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous

forme électronique et que le signataire utilise pour signer » et qui ne respectent pas les exigences eIDAS pour les signatures avancées ou qualifiées.

- ✓ La signature électronique **avancée** est établie de façon plus fiable et permet dès lors de mieux rapporter la preuve devant un juge (Facilité de preuve).
- ✓ La signature électronique **qualifiée** a le même effet juridique que la signature manuscrite. Cette signature électronique qualifiée associe un certificat qualifié eIDAS et un dispositif de création de signature lui aussi qualifié. Un certificat qualifié eIDAS peut s'appuyer sur une Identification Electronique de niveau Substantiel ou Elevé. Les évolutions technologiques en cours et notamment la mise en disponibilité de dispositifs de création de signature électronique qualifiés sur serveurs rend plus facile le déploiement de signatures électroniques qualifiées.

3.1.3 Vérification d'Identité

L'identification du signataire est un élément clé pour l'activation d'une signature électronique et le principal objectif et apport des certificats qualifiés de signature électroniques.

Ceux-ci répondent à des normes techniques ETSI (ES 319 411-2) applicables sur délégation du règlement eIDAS et définissant notamment, en application des critères définis à son article 24.1, les modalités de vérification des identités des signataires. De façon générale, ces dispositions laissent aujourd'hui un pouvoir d'appréciation important aux organismes d'évaluation de la conformité chargés notamment de l'accréditation des prestataires de services de confiance qualifiés (en France Cofrac & LSTI) et ne sont que partiellement harmonisées avec les règles de vérification d'identité des identités numériques eIDAS notamment définies par le règlement d'application UE 2015/1502.

Cette situation atypique – les signatures électroniques eIDAS émises par les prestataires de services de confiance sont juridiquement reconnues de la même manière dans les différents pays de l'Union européenne alors qu'elles reposent sur des règles de vérification d'identité peu harmonisées – apparaît comme une des faiblesses du règlement eIDAS.

La vérification d'identité se fait aujourd'hui essentiellement à distance, une réalité devenue incontournable depuis la pandémie Covid mais non prise en compte dans le règlement eIDAS de 2014. Un effort de clarification important a toutefois été mené en juillet 2021 avec le référentiel ETSI TS 119 461 – Policy and Security requirements for trust services components providing identity proofing of trust services) et, en France, le référentiel PVID ANSSI de mars 2021.

Pour l'identification et la vérification à distance, l'article 24.1 (eIDAS V1) prévoit trois options :

Option 1) A partir d'un moyen d'identification électronique avec garantie de niveau substantiel ou élevé

A l'échelle européenne, 19 pays dont la Norvège et 18 pays de l'UE sur 27 (Autriche, Belgique, Croatie, République Tchèque, Danemark, Estonie, France, Allemagne, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Portugal, Espagne, Slovaquie, Suède), avaient développé et notifié auprès de la Commission Européenne une identité électronique de niveau substantiel et/ou élevé début 2022.

En France, à ce jour, **une seule identité électronique de niveau substantiel** est fournie par La Poste (Identité Numérique de la Poste) ou par France Connect Plus.

Le Service France Connect Plus fonctionne en tandem avec les fournisseurs d'identité ci-dessous :

- *Depuis novembre 2020 :* La Poste (Identité Numérique de la Poste)
- Prévue 2023 : YRIS (avec Mobileconnect et moi - proposé par la Sté AriadNext)
- Prévue pour 2023 : AppCV SESAM VITAL (via Mobile)

- Prévue pour 2023 (niveau Substantiel ET Elevé) : CNIe (Carte Nationale d'Identité électronique) pour la version « document physique » et SGIN (Système de Gestion d'Identité Numérique) pour la version via Mobile

Option 2) Au moyen d'un certificat de signature (ou d'un cachet) électronique qualifié

La liste des prestataires qualifiés est publiée par le Commission Européenne sur la « Trust EU Trust Services Dashboard (europa.eu) » et consultable via le lien suivant :

https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/FR

Option 3) A l'aide de méthodes reconnues au niveau national

- Pour la France l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), définit les exigences et une certification pour encadrer les parcours de vérification en ligne avec le référentiel PVID (Prestataire de Vérification d'Identité à Distance) publié le 1er mars2021. L'ANSSI répond ainsi aux lacunes du texte du règlement d'application 2015/1502 et utilise les prérogatives dévolues aux autorités nationales. L'ANSSI précise les niveaux d'exigences par de nombreuses dispositions supplémentaires.

- Selon les exigences de l'ANSSI, pour obtenir une certification de niveau substantiel, les services doivent présenter deux caractéristiques :
  - Une approche hybride automatique et humaine (l'action humaine étant obligatoire pour chaque vérification d'identité), synchrone ou asynchrone
  - Des solutions de présentation dynamique pour le titre d'identité et le visage de l'utilisateur (à l'aide de vidéos)

- La lecture de puces pour les documents d'identité électroniques est également prise en compte.
- L'ANSSI accepte également les méthodes de « vidéo avec opérateur », si elles sont combinées avec l'utilisation d'un algorithme biométrique dans le processus d'identification à distance. »

- La liste des prestataires PVID certifiés ou en cours de certification est publiée en ligne[4]

Selon les informations publiées, un seul PVID est certifié -Hubble.ai) et une dizaine de projets sont en cours de certification et ont été rendus publics.

- Pour les autres pays de l'Union Européenne, voir les 2 rapports d'ENISA, European Union Agency for Cybersecurity *

! **Remarque :** L'identification du signataire doit bien évidemment se faire dans le respect des textes sur les données nominatives, en particulier du règlement (UE) 2016/679, dit règlement général sur la protection des données (RGPD).

! **En juillet 2021, l'ETSI a publié le standard ESTI TS 119 461 pour la vérification d'identité à distance afin de délivrer un certificat électronique qualifié.**

3.2 Quel niveau de signature choisir ?

Le choix du niveau d'identification et de signature s'effectue e**n fonction du risque financier et juridique**, des réglementations métier (Banque, Assurance, Immobilier, Jeux, Commerce de détail.)

[4] Cf. *https://www.ssi.gouv.fr/entreprise/produits-certifies/prestataires-de-verification-didentite-a-distance-pvid/*

L'ANSSI propose une bonne illustration d'analyse de risque pour le niveau de signature, à laquelle il faut ajouter la friction que pourra engendrer la sécurisation de l'identité du signataire. Schéma ci-dessous.

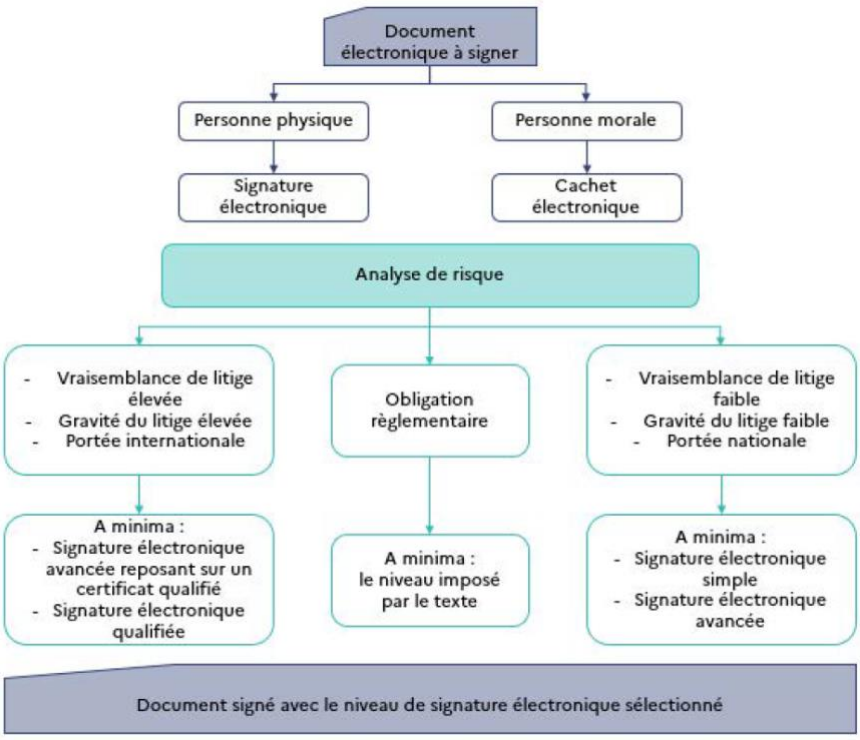


Figure 4 - analyse niveau de signature

Le niveau de signature comporte un certain nombre de caractéristiques dont certaines nécessitaient des éléments matériels. Cette complexité est résolue par l'intégration du certificat électronique dans le cloud.

L'introduction progressive d'ordinateurs personnels et smartphones intégrant, conformément au règlement eIDAS, l'identité numérique de niveau substantiel ou élevé et les certificats qualifiés contribuent fortement à cet objectif.

! **Le Règlement eIDAS, instrument d'application directe en droit interne, est fondamental pour la confiance et propose aux acteurs du marché (citoyens, acteurs économiques et institutions) une boîte à outils qu'ils sont libres de choisir en fonction du niveau de sécurité requis selon les usages.**

Ce règlement établit un cadre d'interopérabilité afin de permettre une reconnaissance mutuelle au sein des Etats membres.

3.3 EUDI Wallet : European Digital ID Wallet

Avec la révision du Règlement eIDAS, la Commission Européenne introduit un nouveau concept : le **Portefeuille européen d'identité numérique** (Digital Identity Wallet DIW)

Présentée le 3 juin 2021[5], Il constitue le principal changement proposé pour la révision eIDAS.

Ce Portefeuille :

- ✓ est destiné à tout citoyen, résident ou entreprise de l'UE

[5] Cf. https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_2663

- ✓ repose sur le principe de maîtrise de leurs données par les utilisateurs
- ✓ et fait un lien entre une identité numérique personnelle et d'autres attributs personnels (dont compte bancaire, diplômes, permis de conduire, …).

Ce portefeuille permettra à son titulaire de signer avec une signature électronique qualifiée,

Avec cette proposition, **plusieurs nouveaux services de confiance** sont évoqués dans les différentes versions du projet :

- ✓ Attributs électroniquement attestés
- ✓ Registres électroniques (sous réserve de confirmation)
- ✓ Dispositif de création de signature électronique (à distance) QSCD
- ✓ Archivage.

La proposition de révision eIDAS devrait être validée en 2023.

- ! Pour l'instant (Juin 2023), il est prévu que les services privés comme **les services financiers,** qui ont un besoin légitime d'authentification forte, **devront accepter l'authentification à travers le portefeuille d'identité numérique si l'utilisateur le souhaite**. A ce jour, il reste un débat sur la généralisation de l'identité numérique sur la totalité des transactions de paiement. (Non justifié pour les paiements par carte à puce). Un champ majeur de réflexion existe pour le cas des paiements à distance

- ! Les banques, dans leur rôle de tiers de confiance, auraient avantage à devenir des émetteurs d'attestations électroniques (Attributs électroniquement attestés), notamment pour les comptes bancaires. Ce qui permettrait de confirmer le lien étroit entre l'IBAN du compte et son propriétaire.

4 Focus Réglementation Bancaire

Les réglementations bancaires sur la lutte contre la fraude et le blanchiment mettent l'accent sur la vérification de l'identité, en particulier à distance.

L'ACPR renforce les exigences sur l'identification lors de la mise en relation à distance pour la conformité LCB/FT en s'appuyant sur eIDAS, et la DSP2 oblige le déploiement de l'authentification forte. Ces exigences bancaires vont dans le même sens que la réglementation eIDAS sur la signature.

4.1 LCB/FT

La solution doit répondre aux règles LCB-FT, à l'analyse circonstanciée des risques et aux attentes « Sans Friction » des marchands.

Conformément aux obligations de vigilance LCB FT dictées par le Code Monétaire et Financier[6], les établissements (financiers, de paiement, de monnaie électronique…) « définissent et mettent en place des dispositifs d'identification et d'évaluation des risques », en tenant compte « des facteurs inhérents aux clients, aux produits, services, transactions et canaux de distribution, ainsi qu'aux facteurs géographiques. ».

Cette obligation de vigilance s'applique à l'Entrée en Relation ainsi que pendant toute la durée de la relation d'affaires (examen attentif des opérations + vérification de leurs cohérences avec la connaissance actualisée de la relation d'affaires).

[6] Cf. Titre VI – Chap.1 / Section 3

L'article R561-5-1 pose le principe d'une entrée en relation par voir électronique en s'appuyant sur un moyen d'identification électronique (MIE) d'un niveau de garantie a minima substantiel à l'échelle européenne. Ce MIE étant suffisant pour garantir la vérification d'identité attendue par les textes.

L'article R561-5-2 traite des exceptions et précise les conditions de conformité de ces mesures de vigilance renforcée, notamment pour **la mise en relation à distance**. Il faut au moins choisir 2 options parmi les suivantes pour la vérification d'identité :

	Choix prévus par l'ACPR	**Implémentation possibles**	**Remarques**
1	Obtenir une copie d'un document officiel en cours de validité comportant sa photographie	Téléchargement copies des pièces avec vérification automatique	Obligatoire depuis le 1/01/2021, source ACPR
2	*Mettre en œuvre des mesures de vérification et de* certification de la copie d'un document officiel *ou d'un extrait de registre officiel par un tiers indépendant de la personne à identifier*		
3	Exiger que le premier paiement des opérations soit effectué en provenance ou à destination d'un compte ouvert au nom du client	Paiement de 1 centime	SCT / SDD / Carte Applicable si un compte (de paiement ou de dépôt) est déjà ouvert.
4	Obtenir directement une confirmation de l'identité du client de la part d'un tiers remplissant les conditions prévues au 1°ou au 2°du I de l'article L. 561-7		
5	Recourir à un service certifié conforme par l'Agence nationale de la sécurité des systèmes d'information, ou un organisme de certification que cette agence autorise au niveau de garantie substantiel des exigences relatives à la preuve et à la vérification d'identité	Référentiel PVID de l'ANSSI*	
6	Recueillir une signature électronique avancée ou qualifiée (ou un cachet électronique avancé ou qualifié) valide reposant sur un certificat qualifié ou avoir recours à un service d'envoi recommandé électronique qualifié comportant l'identité du signataire (ou du créateur de cachet) et délivré par un prestataire de service de confiance qualifié		

Le recours au référentiel du PVID ANSSI pourrait permettre par exemple de faciliter l'enrôlement d'une clientèle qui n'a jamais été bancarisée (ex. jeunes.)

- Il est rappelé que la signature électronique requiert l'utilisation des données personnelles, et selon le RGPD, un consentement pour cette utilisation.
- En contrepoids des obligations de vigilance et de limitation des risques, les acteurs (particuliers, banques, marchands) ont **des exigences** pour faciliter l'utilisation et pour limiter les coûts engendrés par la mise en œuvre de ces obligations règlementaires. Il faudra donc prendre en compte **les coûts** ainsi que **la friction** que peut engendrer, dans certains cas, une signature électronique pour des paiements B2C : consentement RGPD sur l'utilisation des données personnelles en vue d'une signature, Authentification Forte pour les signatures avancées et qualifiées…

4.2 DSP2

La DSP2 (Directive de Services de Paiement 2) vise à améliorer la sécurité des transactions de paiement en ligne et à renforcer les droits des consommateurs. Elle a été adoptée en 2015 et a été transposée dans le droit national des États membres de l'Union européenne (en 2017 pour la France)

Les principales dispositions de la DSP2 sont les suivantes :

1. Mise en place de mesures de sécurité pour protéger les données des consommateurs contre les fraudes
2. **Utilisation d'une autorisation de paiement à deux facteurs pour les transactions en ligne pour renforcer la sécurité**
3. Possibilité pour les consommateurs de révoquer leur autorisation de paiement à tout moment
4. Transparence des frais de transaction pour les consommateurs
5. **Responsabilité partagée entre les commerçants et les établissements de paiement en cas de fraude**
6. Protection des consommateurs contre les paiements non autorisés
7. **Obligation pour les prestataires de services de paiement de mettre en place des procédures pour gérer les réclamations et les litiges de manière efficace**
8. Obligation pour les prestataires de services de paiement de disposer d'un système de surveillance pour détecter les transactions frauduleuses
9. Obligation pour les prestataires de services de paiement de notifier les autorités compétentes en cas de fuites de données ou de fraudes massives
10. Obligation pour les prestataires de services de paiement de respecter les règles de confidentialité et de protection des données.

Les résultats positifs de l'authentification forte sur la baisse de la fraude suite à la mise en place de la DSP2 sont visibles et soulignés dans le dernier rapport de l'Observatoire des paiements.

5 Propositions de solution

5.1 Solution 1 – La signature électronique EBICS en mobilité, ou comment une réflexion du groupe de travail eFinance de la FnTC devient une offre opérationnelle.

5.1.1 Les motivations de l'étude et de sa réalisation.

Faciliter l'usage de la signature électronique dans les transactions bancaires des entreprises est depuis plusieurs années au centre des travaux du groupe de travail eFinance de la Fédération des Tiers de Confiance du numérique. Après avoir promu les solutions interopérables avec l'annuaire ComPac, une réflexion s'est engagée, à la fin de la dernière décennie pour porter les solutions de signature existantes sur tous les types de terminaux. Le but étant d'apporter à la fois l'interopérabilité et la mobilité, en pouvant signer sur n'importe quel type de terminal, poste de travail, tablette, mobile ; fonctionnalité demandée par les utilisateurs professionnels. Parmi les différentes solutions trouvées, la solution analysée ci-après se révèle être compatible avec l'objectif fixé au groupe de travail. Les fonctionnalités prévues dans le projet laissent supposer également que la solution, pourrait être compatible avec le nouveau service proposé en juin 2021 dans le cadre du projet de Règlement eIDAS avec la signature électronique à distance ou « Remote Signature ».

Aujourd'hui, cette solution proposée par la FnTC commence à être prise en compte et intégrée dans les applications bancaires.

Rappelons que la signature électronique a été identifiée très tôt (les premières solutions remontent à 1995 avec ETEBAC 5) comme une solution idéale pour les opérations bancaires professionnelles, qui mettent en risque par les montants et le nombre de transactions très élevés. En effet, il ne s'agit plus de valider une transaction unitaire, comme dans le cas du « retail », mais de valider en une fois un nombre élevé de transactions, par exemple l'envoi des virements de salaire d'une entreprise. Présentant toutes les caractéristiques d'une authentification forte effectuée en amont de sa transmission, les solutions intégrant une signature électronique font l'objet d'une exemption d'authentification forte (au sens de la DSP2) au moment de la transaction (exemption article 17 DSP2 https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/2eme-directive-sur-les-services-de-paiement). Pourtant, la mise en œuvre, qui se veut la plus interopérable possible,

présentent des limites de confort et de sécurité avec l'utilisation de solutions Token USB sur les postes de travail et leur réutilisation sur d'autre types de terminaux.
C'est pourquoi le groupe de travail de la FnTC a très tôt et bien avant la publication des propositions d'évolution du règlement eIDAS par la Commission Européenne, axé une des recherches de solution qui soit basée sur la délocalisation de l'environnement de signature et sur l'authentification du signataire par l'identité numérique. Pour assurer l'interopérabilité et atteindre le niveau qualifié eIDAS en matière de signature électronique, il était également nécessaire de recourir à des interfaces standardisées ou normalisées.

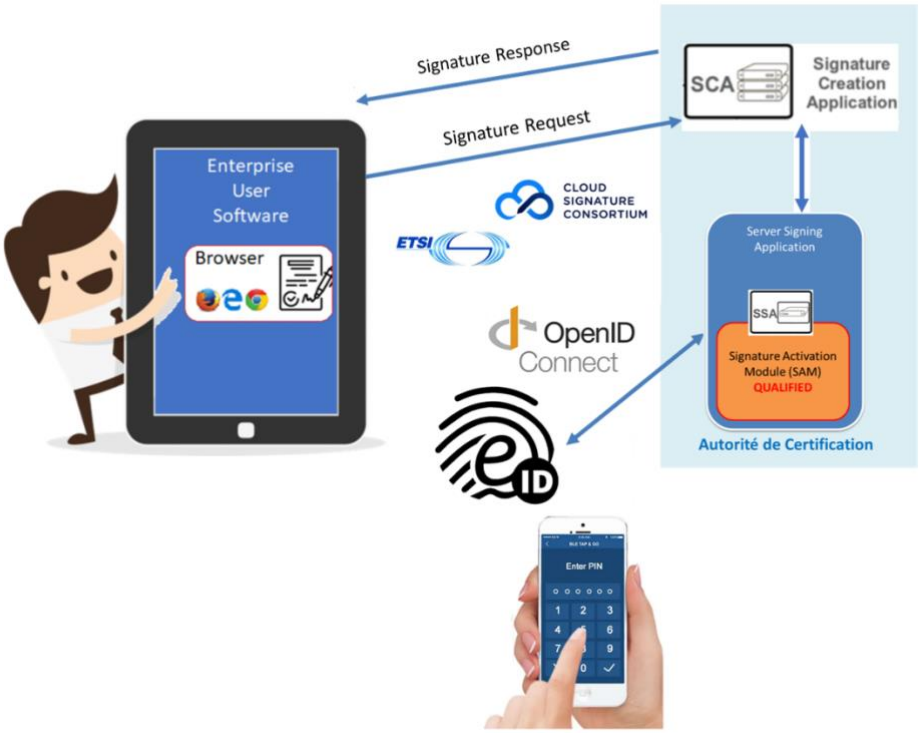
5.1.2 La réalisation.

Grâce à la pluralité des acteurs intervenant dans le GT eFinance de la FnTC, Autorités de Certification, Editeurs de logiciels, Communauté d'utilisateurs et de prescripteurs, et comme évoqué dans le paragraphe précédent, une des propositions élaborée et présentée par le groupe de travail est basée sur :

- Une authentification du signataire avec une identité électronique de niveau substantiel ou élevée eIDAS.
- Un environnement de création de signature (QSCD Qualified Signature Creation Device) qualifié eIDAS hébergé dans un module cryptographique sécurisé du type HSM (Hardware Security Module) sous le contrôle de l'Autorité de Certification, AC.
- Un Module d'Activation également qualifié eIDAS (SAM Signature Activation Module) également déporté au niveau de l'environnement de création de signature chez l'AC.
- Le recours à des protocoles d'échanges standardisés/normalisés pour la communication du fichier, ou plus exactement à son condensat, hash, à signer, comme le protocole ETSI 119 432 proposé par le CSC, Cloud Signature Consortium.
- Le recours à des protocoles standardisés/normalisés pour activer l'authentification du signataire par son identité électronique comme OpenID Connect, OIDC, qui utilise les mécanismes d'autorisation et d'authentification d'OAuth 2.0.

Avant de pouvoir signer, l'utilisateur devra, comme pour toute opération de signature électronique, s'enrôler auprès d'un fournisseur d'identité électronique qualifié eIDAS (et notifié pour bénéficier d'un passeportage européen), auprès de l'Autorité de certification avec son identité électronique pour se faire délivrer un certificat de signature qualifié eIDAS et dans le progiciel qui utilisera la signature électronique à distance (Remote Signature). Après cette phase d'enrôlement à effectuer une seule fois, la signature électronique, de niveau qualifié eIDAS, sera possible pour toutes les transactions. Il est à noter, que les enrôlements sont également basés sur de l'authentification avec une identité électronique, simplifiant ainsi le parcours client qui se déroule entièrement à distance. Le pivot sécuritaire est l'identité électronique, qui sera obligatoirement de niveau substantiel ou élevé.

La partie signature se résume sur le schéma ci-après :



5.1.3 Bilan et enseignements

Déjà utilisée depuis de nombreuses années pour les ordres de paiement en provenance des professionnels, la signature électronique devrait connaître une nouvelle montée en charge avec la diffusion et l'utilisation de l'identité électronique combinée avec la facilité apportée par les dispositifs de création de signature qualifiés à distance.
Cette nouvelle déclinaison commence à être intégrée dans les offres de plusieurs Autorités de Certification et éditeurs de logiciels bancaires, et devrait séduire l'ensemble des banques par son acceptation qui ne demande aucun développement du côté des serveurs bancaires. En effet, l'opération de signature est effectuée avant la transmission de l'ordre à la banque qui reste ainsi totalement inchangée. Sa conformité avec la Signature Qualifiée eIDAS, facilite l'acceptation par les établissements financiers.
Enfin, cette solution devrait également pouvoir, d'une part se décliner à d'autres usages de signature électronique, comme de la signature de contrats et pourrait également intéresser le secteur du paiement retail en proximité comme à distance mais avec quelques développements complémentaires pour parfaire le parcours client de paiement comme associer un jeton obtenu lors de l'identification/authentification d'entrée sur le service et réutilisé au moment de la signature du paiement.

5.2 Solution 2 – Signature d'un paiement

Cette signature doit permettre de gérer les preuves du consentement.

Les preuves concernant un consentement sur un parcours numérique sont constituées d'éléments provenant de différents acteurs (machines ou humains) et peuvent contenir des éléments du parcours préalables au consentement final.

Un parcours de paiement est un parcours digital qui se finalise par un consentement sur un paiement.

La validation du paiement par le Payeur est la concrétisation de son consentement.

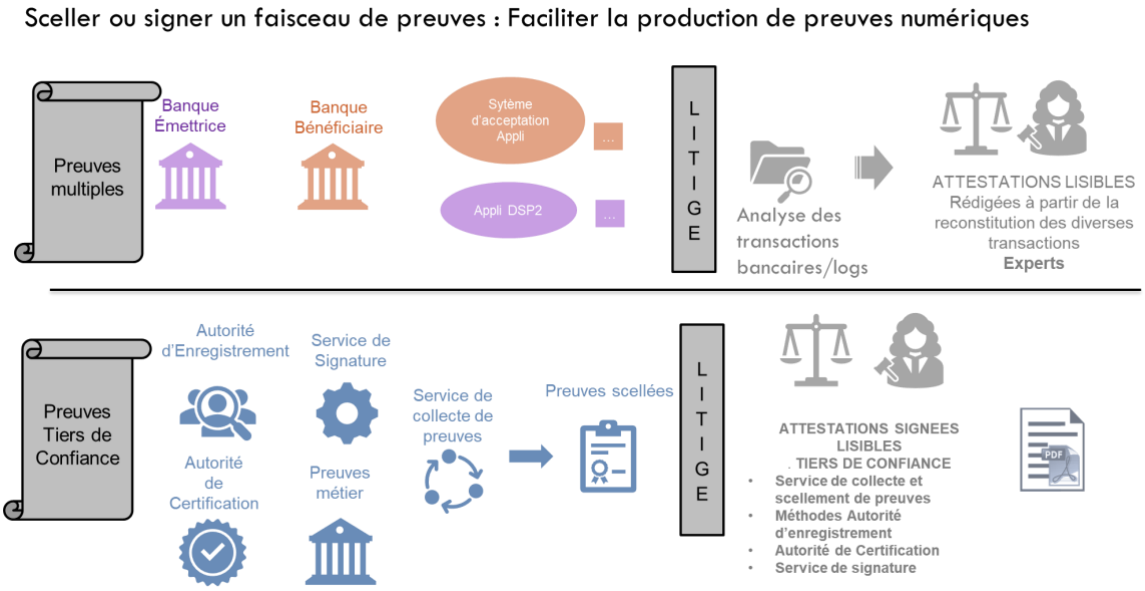
Lors d'un litige « Payeur », il faut que la banque du Payeur émette des preuves lisibles. Or les preuves d'un paiement proviennent de plusieurs tiers et souvent sous forme de données informatiques.
les dossiers de preuves sont un ensemble de champs des messages échangés pour la transaction

bancaire en cours (technique) accompagné d'attestation lisible rédigées avec une reconstitution lisible des divers messages constituant la transaction de paiement. Parfois des experts doivent intervenir. Le coût d'un litige peut donc être très coûteux en ressources humaines.

Si les preuves sont collectées et scellées par un tiers de confiance au moment de l'utilisation du moyen d'authentification forte (DSP2) fourni par l'application mobile de la banque du Payeur, elles permettront l'émission d'une attestation qui restituera l'intégralité de la cinématique de la transaction ainsi que des données complémentaires collectées par cette application mobile. Cette fonctionnalité est déclenchée en fonction de la gestion du risque de la banque du Payeur.

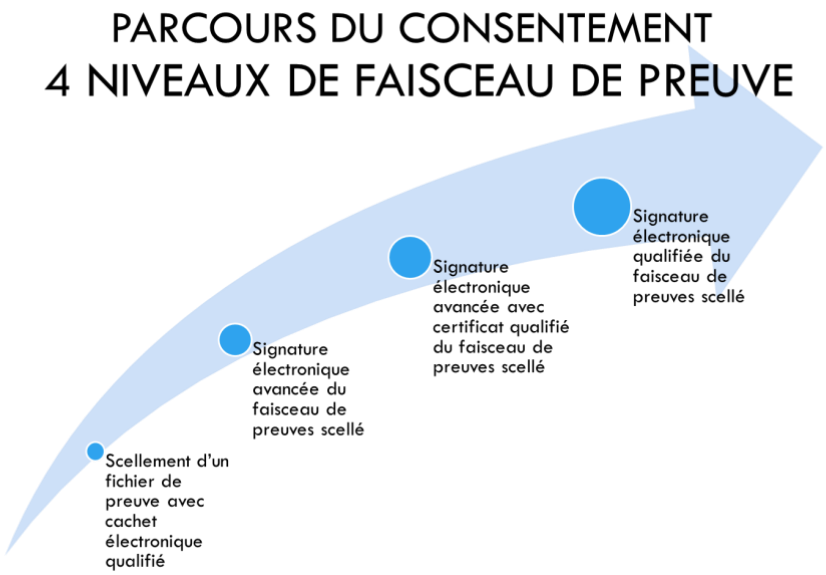
En effet la plupart des applications bancaires intégrant l'authentification forte enregistrent les données de la transaction, exemples :

- ✓ Niveau d'identification
- ✓ Type d'authentification
- ✓ Transaction bancaire : n° de transaction, montant, date de la validation…
- ✓ Émetteur : dénomination/nom-prénom, BIC IBAN
- ✓ Bénéficiaire : dénomination/nom-prénom, BIC IBAN
- ✓ Mobile : OS, Marque, modèle, géolocalisation, empreinte du mobile, adresse IP….



Les services Tiers de Confiance fournissent des attestations lisibles qui retracent l'ensemble du service fourni.

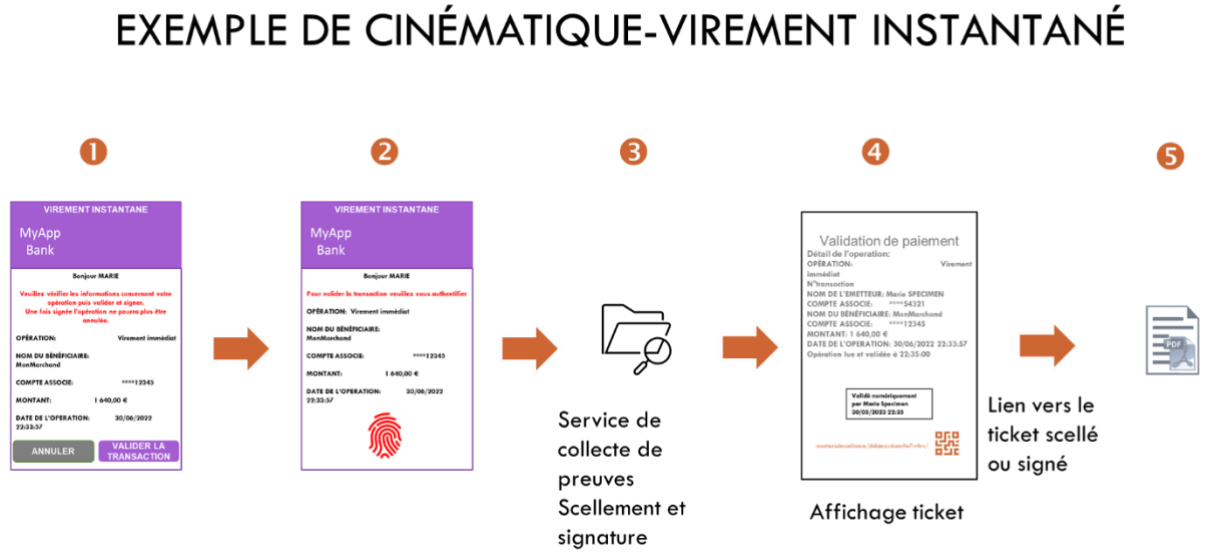
4 niveaux de preuves sont possibles. Le 1er niveau est un scellement de faisceau de preuves.



Le niveau de preuves choisi dépend sur risque porté par la transaction de paiement.

Des travaux sont en cours à la FNTC en vue d'une harmonisation de la collecte et restitution des preuves de consentement d'un parcours numérique (plus large que le paiement) pour assurer des bonnes pratiques en vue d'une meilleure interopérabilité des faisceaux de preuves.

La solution proposée est d'intégrer une fonctionnalité de gestion de la preuve, initiée avec le niveau choisi en fonction du risque.



La collecte du faisceau de preuves pour une transaction de paiement s'effectue au travers du moyen d'authentification forte (DSP2) mis à disposition par la banque du payeur au payeur. Le résultat un ticket récapitulatif PDF et son faisceau de preuves scellés ou signés.

Cette solution facilite également la recherche des transactions et des logs si des approfondissements sont nécessaires.

Cette solution permet l'émission d'une attestation avec les éléments preuves de la transaction de paiement et un ticket scellé ou signé.

Cette solution peut s'intégrer dans n'importe quel parcours ou transaction numérique.

Conclusion

La révision du Règlement eIDAS en cours d'approbation, introduit des innovations majeures, dont la mise en place d'un **portefeuille européen d'identité numérique** (Digital Identity Wallet DIW). Cette innovation à caractère universel, et pourrait s'appliquer à long terme à l'ensemble des paiements numériques et notamment à plus court terme aux paiements à distance. Nous verrons ce qu'il en adviendra après les votes, notamment au Parlement européen et au Conseil européen.

Le mix sécuritaire d'une identité numérique et d'une signature électronique offrirait une garantie plus importante aux transactions de paiement par une réponse juridique et technique de haut niveau. La démonstration a été faite plus haut. Et il serait possible de bâtir rapidement des solutions viables aux plans économique et technique.

Mais, avant d'engager des investissements très lourds pour les acteurs du paiement, et un nouveau « mode » de paiement pour les particuliers, il faut se poser cas par cas, la question de l'opportunité et des contraintes. Et il faut prendre en compte de nombreux paramètres.

Ainsi, dans tous les cas, la règlementation indique à la fois que :

- Les banques (et de façon générale, tous les PSP) doivent analyser les niveaux de risques des transactions réalisées par les clients et adapter leurs moyens aux risques générés,
- Les acteurs économiques sont en droit de soulever des questions de friction dans les transactions commerciales et de paiement, et de coût des solutions sécuritaires, au regard des montants payés.

Plusieurs autres paramètres doivent être pris en compte :

- L'existence de solutions sécuritaires jugées jusque-là pertinentes pour diverses transactions de paiement, comme la puce pour les paiements par carte de proximité (face à face), ou l'authentification forte pour les opérations à distance,
- Les volumes, et bien sûr les montants, des transactions réalisées : il est clair qu'en phase de lancement d'un nouvel instrument, des mesures sécuritaires élevées nuisent à son adoption par les acteurs du paiement,
- Les investissements qu'il convient de réaliser pour une nouvelle solution sécuritaire et le respect d'un level playing field entre les PSP, au moins au niveau européen,
- Les innovations technologiques, qui peuvent offrir de nouveaux moyens aux fraudeurs, notamment en termes de capacité des algorithmes et des ordinateurs,
- Les technologies envisagées pour le Portefeuille européen, et leur adaptation au monde du paiement.

Il reste que :

- Au plan européen, la numérisation généralisée des transactions de paiement, et de développement des crypto-paiements imposera une identité numérique européenne pour les paiements.
- Cette identité pourrait être gérée de façon décentralisée par les PSP, ce qui permettrait de confirmer leur rôle de tiers de confiance du numérique mais la règlementation devra alors instituer un Level playing field que tous les PSP se dotent de moyens équivalents et interopérables d'identité numérique pour leurs clients.
- Avec le développement du virement instantané, et demain de l'euro numérique, l'exigence sécuritaire va s'amplifier. Déjà la question de la « confirmation of payee » se pose pour le virement instantané, alors que les volumes sont encore très faibles.

Diverses stratégies peuvent être envisagées :

- Peut-être cibler les instruments prioritaires, et en l'occurrence, le virement instantané pourrait être le premier instrument concerné par un accroissement substantiel des moyens de sécurisation des transactions et de lutte contre la fraude
- Cibler les types de transactions prioritaires, comme les transactions internationales ou les transactions B2B, ou les transactions B2C ou P2P de grand montant…
- Il faut dans tous les cas, prendre en compte **les coûts des transactions** ainsi que **la friction** que peut engendrer ces nouvelles solutions.

Avis de FRANCE PAYMENT FORUM

La sécurité est la clé du développement des paiements numériques, et la DSP l'a bien pris en compte, en faisant de la sécurité des paiements une question centrale, notamment avec l'authentification forte. Mais, cinq ans après la DSP2, malgré des progrès majeurs en ce domaine, la question de la sécurité des paiements numériques restent une question d'actualité et les divers comités et organismes concernés en France et en Europe pour lutter contre la fraude dans les paiements tentent d'y apporter des solutions pérennes.

FRANCE PAYMENTS FORUM souhaite qu'il y ait en ce domaine de la sécurité des paiements un saut qualitatif au plan européen, et au moins au plan national, à la fois pour opposer une réponse forte aux fraudeurs et assurer ainsi le développement des paiements numériques, pour se préparer à couvrir les nouveaux risques liés aux nouveaux instruments et modes de paiement numériques, et ceux liés aux évolutions technologiques, comme l'IA ou le déploiement des ordinateurs quantiques. La priorité est donc dans les paiements à distance, et pour la France, dans les paiements par chèque qui perdurent et constituent le premier gisement de la fraude dans les paiements.

Pour les paiements à distance, la Signature électronique et l'identité numérique constituent des solutions efficaces et de futur, qu'il convient désormais d'envisager sérieusement, à côté d'autres solutions, comme la tokenisation et la biométrie, Et plusieurs évolutions règlementaires et techniques contribuent à assurer leur simplicité de mise en œuvre, leur validité juridique et la baisse de leurs coûts. Le présent Document de position fait un point complet de ces solutions, qui éclaire bien leurs apports et leur opportunité de mise en œuvre, à court et moyen terme.

Mais, aujourd'hui, face à l'amoncellement des investissements nécessaires, il faut cibler ce saut qualitatif à court terme sur les domaines prioritaires, et éviter d'empiler les couches sécuritaires, là où des réponses satisfaisantes et efficaces existent depuis de nombreuses années, comme dans les paiements de face à face avec la carte bancaire.

La stratégie à mettre en œuvre doit déjà permettre de distinguer les paiements d'entreprises, et les paiements de particuliers, et dans ce dernier cas, permettent d'amortir les investissements réalisés dans la dernière période avec l'authentification forte, et la compléter dans les divers cas où la certification électronique, la signature électronique ou l'identité numérique apportent des solutions concrètes et rapides.

Mais, il faut également préparer le futur, avec une généralisation de ces solutions pour les paiements numériques à distance, et le déploiement de ces solutions nécessitent à la fois un investissement important et un scénario de mise en œuvre.

FRANCE PAYMENTS FORUM souhaite qu'il y ait en Europe, et au moins en France, une réflexion majeure sur les apports de ces solutions et leurs points d'application les plus tangibles dans les paiements, en distinguant bien les paiements de particuliers et ceux des entreprises, Et pour définir une stratégie de lutte contre la fraude à 5 ou dix ans prenant en compte leurs apports. Et ils souhaitent que ces solutions soient de préférence européennes et spécifiques aux paiements à la fois pour assurer une adhésion large à ces solutions, par leur pertinence, leur efficacité et leur respect de la confidentialité, et un déploiement massif de ces solutions, mais étalé sur moyenne et longue période, avec un modèle économique adapté, comme ce fut le cas pour le lancement de la carte à puce. Ce document de position a pour objet de contribuer à ces réflexions.

Avis de la FnTC

Impliquée depuis sa création en 2001 dans la problématique et la promotion des applications de la signature électronique, la Fédération des Tiers de Confiance du Numérique a publié plusieurs guides téléchargeables sur ce sujet et ses domaines connexes comme son archivage, l'archivage des preuves et son environnement juridique et réglementaire, notamment avec eIDAS, qui ont été largement évoqués dans ce document.

En ce qui concerne le paiement, la démarche menée avec succès par la FnTC en abordant le paiement par les cas d'usage concernant les applications professionnelles pourraient se décliner vers des applications C2C ou C2B, y compris C2Gov, non seulement dans le domaine du paiement, mais aussi de tous les cas d'usages couverts par la signature électronique.

Si c'est bien la convergence de l'identité numérique et de l'évolution de la réglementation européenne attendue dans les toutes prochaines années avec la future version du règlement eIDAS, son concept de portefeuille de services qualifiés associés à l'identité numérique, qui vont apporter une nouvelle diffusion de la signature électronique auprès du citoyen européen que ce soit dans son application personnelle comme professionnelle, c'est aussi le choix d'une approche associée à l'usage de la standardisation et de la normalisation qui ont fait le succès de cette démarche..

C'est pourquoi ce groupe de la FnTC travaille maintenant sur l'intégration dans le portefeuille EUDIW du règlement eIDAS tout en travaillant, avec les autres Groupes de Travail de la FnTC, sur les déclinaisons professionnelles de l'Identité et de la dématérialisation du KYC, étape nécessaire à la simplification de la partie enrôlement, point d'entrée qui doit impérativement être fluide pour la réussite de l'ensemble des opérations.

Ce premier document rédigé avec France Payment Forum, doit être vu comme le point de départ d'une synergie à venir entre les experts de France Payment Forum et ceux de la FnTC pour imaginer des nouvelles solutions applicables, au moins dans la zone euro, à la problématique et aux attentes des professionnels comme des particuliers, en matière de paiement et dans le respect des réglementations, des standards et de l'accroissement de la sécurité afin de diminuer la fraude néfaste à tout l'eco-système.

Annexe 2 - Bibliographie et Références

Observatoire de la Sécurité des moyens de paiement – Rapport Annuel 2021	www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021
ACPR Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle. Elaborées par l'Autorité de contrôle prudentiel et de résolution (ACPR), elles sont destinées aux organismes financiers soumis à son contrôle. Décembre 2021	https://acpr.banque-france.fr/sites/default/files/media/2022/05/11/20220404_lignes_directrices_revisees_relatives_identification_verification_connaissance.pdf
GUIDES FnTC – CR2PA Signature Electronique I, II et III », trois fascicules didactiques qui précisent les règles à appliquer pour chacune des phases de la signature, de la phase préalable à l'archivage 2022 et 2023	LaSignatureElectronique_Definiti.pdf (fntc-numerique.com) fntc_signatureelectronique_ii.pdf (fntc-numerique.com) Signature-electronique-3.pdf (fntc-numerique.com)
GUIDE FnTC Guide des bonnes pratiques pour maîtriser et optimiser la connaissance client. Aout 2021	https://fntc-numerique.com/upload/file/guides-fntc/fntc_kyc.pdf
GUIDE ANSSI Guide de sélection du niveau de signature et de cachet électronique Décembre 2021	anssi-eidas-guide-niveau-signature.pdf
COMMISSION EUROPEENNE – EU Trust Services Dashboard Liste des prestataires, à l'échelle européenne, avec une offre de services de Signature (et/ou de Cachet) électronique qualifié(e), conformément à la réglementation eIDAS V1.	https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
COMMISSION EUROPEENNE Révision eIDAS pour une « identité numérique fiable et sécurisée pour tous les Européens » présentée le 3 juin 2021	*https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_2663*
EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA Analysis of methods to carry out identity proofing remotely Mars 2021 (Version en anglais)	https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing
Code Monétaire et Financier Articles R 561-5-1 et R 561-5-2	https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041577229
Règlement eIDAS	https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=hr