Forum Fintech ACPR-AMF

Groupe de travail sur la vérification d'identité à distance des personnes physiques

Compte-rendu des travaux

Ce compte rendu retrace les réflexions du groupe de travail réunissant des représentants de fédérations professionnelles, d'établissements bancaires, de prestataires de service de vérification d'identité et d'autorités publiques concernées. Il ne saurait engager l'ACPR ou l'AMF.

Synthèse du groupe de travail

Dans le cadre du Forum Fintech ACPR-AMF, **un groupe de travail sur l'identification des personnes physiques à distance** a été constitué avec les acteurs de place : entre mars et juin 2019, il a réuni des représentants de fédérations professionnelles, d'établissements bancaires, de prestataires de service de vérification d'identité et d'autorités publiques concernées. **Son objectif était d'établir un diagnostic précis des difficultés** rencontrées par les établissements financiers lors de l'entrée en relation à distance avec leurs clients et **d'évaluer les solutions possibles** au regard des exigences pratiques propres à ce mode d'entrée en relation et des niveaux de sécurité requis compte tenu des risques de blanchiment et de financement du terrorisme.

De fait, **dans de nombreux pays de l'Union Européenne**, la prise en compte des nouvelles technologies de vérification d'identité à distance lors de la transposition la 4ème directive LCB-FT semble avoir ouvert aux banques **un éventail de moyens d'identification plus large qu'en France**. Le Code monétaire et financier ne reconnaît, comme équivalent au face-à-face lors de l'entrée en relation, que le recours à l'identité électronique de niveau élevé, au sens du règlement européen eIDAS. À défaut, il exige l'utilisation de deux mesures de vigilances complémentaires parmi six disponibles depuis octobre 2018. Or, il apparaît que **les solutions d'identité électronique de niveau élevé** - aujourd'hui seulement atteignables par des institutions publiques – **ne sont pas disponibles** et ne sont pas susceptibles d'être utilisées à grande échelle par les acteurs financiers à court ou moyen terme. Quant aux **mesures de vigilances complémentaires**, de nature et de niveau de sécurité inégaux, celles les plus susceptibles de **promouvoir des techniques d'entrée en relation sécurisées et à l'état de l'art** se voient en pratique handicapées par une **durée de certification trop longue** et une articulation avec les autres mesures complémentaires qui réduit leur intérêt en termes de parcours client.

Les travaux du groupe montrent qu'**il est possible techniquement de proposer des parcours clients plus fluides et intuitifs tout en maintenant un niveau de sécurité équivalent au face-à-face**. Pour les rendre possibles juridiquement, et tout en maintenant la **cohérence forte de la réglementation financière française avec les normes de sécurité eIDAS**, le groupe a identifié un certain nombre de propositions de modifications réglementaires, principalement de niveau infra-législatif.

Le groupe a constaté en premier lieu que le niveau substantiel du règlement eIDAS a été conçu pour offrir le même niveau de sécurité qu'un face-à-face avec une personne physique raisonnablement formée, sans être spécialiste de la vérification d'identité. Aussi le groupe de travail préconise-t-il de **considérer comme équivalent au face-à-face le niveau de garantie substantiel pour la vérification d'identité électronique, sans appeler aucune mesure de vigilance complémentaire [proposition 1]**. En pratique, cette disposition est susceptible d'encourager le développement des solutions d'identification de niveau substantiel, dont plusieurs devraient être, à court terme, disponibles sur le marché français.

En remplacement de la cinquième mesure de vigilance complémentaire actuelle (R. 561-20), le groupe de travail **propose de permettre toute solution technique qui, sans être certifiée de niveau substantiel au sens de l'eIDAS, offre un module de « vérification d'identité » équivalent** techniquement à celui requis pour le niveau substantiel. L'utilisation d'une telle solution en conjonction avec la première mesure complémentaire permettait de **réduire, dans ce cas, les pièces justificatives demandées au titre de cette première mesure** sans abaisser le niveau de sécurité. Pour assurer en pratique l'équivalence recherchée, il est proposé d'imposer la conformité de ces solutions aux **extraits pertinents du référentiel** d'exigences de sécurité sur les moyens d'identification électronique de niveau substantiel **de l'ANSSI** [proposition 2.1]. La conformité des solutions à ce « nouveau » référentiel serait évaluée sur une périodicité de 2 ans par un tiers indépendant certifié par l'ANSSI [proposition 2.2].

Le groupe de travail propose par ailleurs d'**inclure l'envoi recommandé électronique au sein de la sixième mesure de vigilance complémentaire** [proposition 3].

Lors de ses travaux, le groupe a constaté l'absence de données factuelles permettant de comparer les niveaux de sécurité des différents processus d'entrée en relation à distance et des entrées en relation en face-à-face. L'ouverture éventuelle à un plus large éventail de solutions techniques d'entrée à distance accroîtra le besoin de s'assurer, ex-post, du niveau effectif de sécurité du marché français, en particulier au regard dans le contexte de la lutte contre le blanchiment et le financement du terrorisme (LCB-TT). Aussi est-il proposé de mettre en place un ***reporting*** des données les plus à même d'établir un suivi minimal du niveau de sécurité des entrées en relation, physiques et à distance [proposition 4].

Enfin, le groupe de travail a observé que **l'article R. 312-2** du code monétaire et financier énonçait – pour les établissements bancaires seulement – des exigences légèrement différentes et supplémentaires de celles de l'article R. 561-20. Ces **exigences supplémentaires sont susceptibles d'alourdir le processus d'entrée en relation à distance**, sans pour autant renforcer le niveau de sécurité du dispositif LCB-FT des banques. C'est pourquoi le groupe de travail **propose qu'en soit étudiée la suppression** [proposition 5].

Les propositions évoquées ci-dessus ne constituent qu'un socle de réflexion pour une évolution possible du cadre réglementaire en vigueur. Des solutions alternatives sont discutées dans le présent rapport. Toutefois, les pistes retenues ont paru les plus intéressantes au groupe : tout en maintenant un niveau de sécurité de haut niveau, elles semblent pouvoir introduire la souplesse et la proportionnalité nécessaire au développement d'un écosystème plus mature et efficace pour la vérification d'identité à distance, à l'instar d'autres pays de l'Union Européenne.

Table des matières

I. État des lieux de la vérification d'identité à distance

A. Le cadre réglementaire français de la vérification d'identité à distance permet une flexibilité d'appréciation

Parmi les normes internationales, la réglementation sur la connaissance client à distance, dans laquelle est inclue la vérification d'identité, doit tenir compte des recommandations du Groupe d'action financière (GAFI), organisme intergouvernemental de lutte contre le blanchiment et le financement du terrorisme[1]. Les recommandations du GAFI indiquent que les « *relations d'affaires ou opérations qui n'impliquent pas la présence physique des parties* » causent des risques potentiellement plus élevés appelant le cas échéant des mesures de vigilance renforcées[2].

Par ailleurs, le cadre réglementaire français doit assurer la transposition de la 4e directive européenne relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme dit « 4e directive LCB-FT ». Cette directive de 2015 a été modifiée par une nouvelle directive de 2018 (dite « 4e directive révisée LCB-FT » ou « 5e directive LCB-FT »), dont la transposition en droit national doit intervenir au plus tard le 10 janvier 2020. Cette directive dans sa version modifiée prévoit que « *les relations d'affaires ou transactions qui n'impliquent pas la présence physique des parties et qui ne sont pas assorties de certaines garanties »* telles que des moyens d'identification électronique*, des services de confiance pertinents au sens du règlement (UE) no 910/2014 ou tout autre processus d'identification sécurisé, électronique ou à distance, réglementé, reconnu, approuvé ou accepté par les autorités nationales concernées »* constituent un facteur de risque potentiellement plus élevé appelant des mesures de vigilance renforcées à l'égard de la clientèle. Les autorités européennes de supervision[3] ont publié en juin 2017 des lignes directrices sur les facteurs de risque. Celles-ci confirment que les « *non-face-to-face business relationships, where no adequate additional safeguards – for example electronic signatures, electronic identification certificates issues in accordance with Regulation EU (No) 910/2014 and anti-impersonation fraud checks – are in place* » peuvent constituer un facteur de risque plus élevé. Ces lignes directrices sont en cours de révision.

Les normes internationales et européennes posent des principes clairs mais confèrent aux autorités nationales des marges de manœuvre pour leur application. Dans ce contexte, des choix de transposition ont dû être faits pour déterminer le cadre réglementaire français et ont abouti au décret du 18 avril 2018[4] entré en application le 1er octobre 2018. En dehors des dispositifs

[1] Pour information, dans le cadre du GAFI, la France sera évaluée par ses pairs en 2020.

[2] Recommandations du GAFI de 2012, mises à jour en octobre 2018, note interprétative de la recommandation 10 portant sur le devoir de vigilance relatif à la clientèle. Le GAFI précise cependant qu'il s'agit là d'indicateurs utiles et non pas d'éléments contraignants de ses normes. Par ailleurs, le GAFI estime que les « *opérations n'impliquant pas la présence physique des parties* » peuvent être une circonstance « *où il pourrait être permis d'achever les obligations de vérification [d'identité] après l'établissement de la relation d'affaires* ».

[3] Il s'agit de l'Autorité européenne bancaire (EBA), de l'Autorité européenne des marchés financiers (ESMA) et de l'Autorité européenne des assurances et des pensions professionnelles (EIOPA).

[4] Décret n° 2018-284 du 18 avril 2018 renforçant le dispositif français de lutte contre le blanchiment de capitaux et le financement du terrorisme

d'identification électronique équivalents au face-à-face – qui sont en réalité indisponibles à ce stade, la réglementation française demande que les établissements financiers appliquent des mesures de vigilance complémentaires pour les entrées en relation à distance, lorsque « *le client ou son représentant légal n'est pas physiquement présent aux fins de l'identification au moment de l'établissement de la relation d'affaires* » (L. 561-10 Code Monétaire et Financier). La liste des mesures de vigilance complémentaire admises est donnée à l'article R. 561-20 du Code Monétaire et Financier.

B. Les équivalents au face-à-face pour la vérification d'identité sont en pratique indisponibles

Habituellement, après avoir identifié leurs clients (recueil du nom et prénoms ainsi que date et lieu de naissance pour les personnes physiques, recueil de la forme juridique, de sa dénomination, de son numéro d'immatriculation et de l'adresse du siège social pour les personnes morales)[5], les établissements financiers vérifient l'identité de leurs clients par la présentation d'un document officiel d'identité avec photographie pour les personnes physiques (3° de l'article R. 561-5-1 du CMF) et par la communication de l'original ou de la copie de tout acte ou extrait de registre officiel datant de moins de trois mois pour les personnes morales (4° du R. 561-5-1). Sinon, ils appliquent deux mesures de vigilance complémentaires parmi celles listées à l'article R. 561-20.

Désormais, dans le cadre d'une entrée en relation à distance, si l'établissement financier recourt à un moyen d'identification électronique de niveau de garantie élevé au sens du règlement (UE) 910/2014 « eIDAS » (1° du R. 561-5-1) ou à un moyen d'identification électronique présumé fiable au sens de l'article L. 102 du code des postes et des communications électroniques, CPCE (2° du R. 561-5-1), il n'est pas attendu que l'établissement mette en œuvre des mesures de vigilance complémentaires. Des projets sont en cours pour offrir ces dispositifs d'identification électroniques équivalents au face-à-face en France, mais à l'heure actuelle aucun dispositif de ce type n'est disponible.

Il y a d'une part le projet ALICEM porté par l'Agence nationale des titres sécurisés (ANTS) qui reposera sur le passeport biométrique et les smartphones Android et qui postule pour le niveau de garantie élevé (pré-notification attendue à fin 2019 selon l'ANSSI étant noté que la notification ne peut intervenir qu'après revue par les pairs et avis du réseau de coopération ce qui prendrait au moins 6 mois), limitant la population résidente en France couverte. Il y a d'autre part l'identité numérique de niveau élevé que cherche à construire le programme interministériel d'identité numérique dirigé par Valérie Peneau lancé en janvier 2018[6]. La stratégie pour parvenir à construire et à déployer ce moyen d'identification, qui pourrait être une carte d'identité électronique, n'est pas encore définie. Le groupe de travail estime toutefois que son déploiement prendrait encore plusieurs années, probablement plus de cinq ans. Par ailleurs, aucun équivalent au face-à-face pour les personnes morales ne semble envisagé, alors que les moyens d'identification électronique de niveau

[5] R561-5 du code monétaire et financier

[6] Lettre de mission du Ministre de l'intérieur, de la Garde des Sceaux et du Secrétaire d'État chargé du numérique du 5 janvier 2018 à Madame Valérie Peneau.

élevé au sens d'eIDAS ou présumés fiables au sens du CPCE peuvent en droit concerner les personnes morales.

Si des moyens d'identification de niveau de garantie élevé sont disponibles dans d'autres pays européens, il n'est pas démontré que ceux-ci soient utilisés aux fins de la vérification d'identité par les établissements bancaires. Une douzaine de pays aurait notifié à la Commission Européenne un schéma d'identification[7]. La plupart de ceux-là reposeraient sur une pièce d'identité électronique à l'exception de l'Italie et du Royaume-Uni. L'Allemagne dispose d'un schéma d'identification électronique de niveau élevé notifié en 2017 (carte nationale d'identité et permis de séjour électronique). Il semblerait toutefois que moins de 2% de la population en soit titulaire. Le schéma d'identification britannique de niveau élevé ne serait également pas largement déployé. Par ailleurs, les membres du groupe de travail s'interrogent sur l'accessibilité de ces schémas d'identification étrangers aux résidents français comme par exemple l'e-résidence proposée par l'Estonie. Un panorama des systèmes d'identité en Europe et de leur utilisation par le monde bancaire, consolidé par la Fédération Bancaire Européenne, figure en annexe de ce document.

En revanche, en Allemagne, une circulaire de la BAFIN reconnaît un processus de vidéo-identification comme équivalent au face-à-face, à condition de respecter les exigences énoncées dans une circulaire. Celle-ci a été plusieurs fois révisée depuis sa première version de 2014 (la dernière version date de 2017 -Circular 3/2017). Il convient toutefois de noter que dans un communiqué du 26 mars 2019, le superviseur allemand a appelé l'attention sur le risque de fraude dans les procédés d'identification par vidéo (ex : de faux entretiens d'embauche en parallèle desquels un système ouvrirait un compte au nom du candidat à son insu).

C. Des mesures de vigilance complémentaires aux performances inégales

La liste limitative des mesures de vigilance complémentaires a été révisée par le décret du 18 avril 2018 pour désormais comprendre six mesures de vigilance complémentaires énoncées au R. 561-20 du code monétaire et financier. Les établissements doivent en appliquer au moins deux parmi les six pour vérifier l'identité de leurs clients à l'entrée en relation. Les quatre premières sont issues d'un décret de 2009 transposant la 3e directive européenne LCB-FT (2005). Nécessaires pour les acteurs financiers comme non-financiers assujettis aux obligations de LCB-FT, elles ont été légèrement remaniées par le décret du 18 avril 2018. La cinquième et la sixième sont en revanche de nouvelles mesures de vigilance complémentaires. Il s'agit (i) d'un moyen d'identification électronique avec un niveau de garantie substantiel au sens d'eIDAS et (ii) d'une signature/cachet électronique de niveau avancé ou qualifié reposant sur un certificat qualifié.

Il semble que tous les pays n'aient pas fait le choix de donner une liste limitative de mesures de vigilance renforcées à appliquer pour les entrées en relation à distance. D'autres pays demandent des mesures de vigilance renforcées mais laissent les établissements financiers décider du contenu de ces mesures. Ce choix plus ouvert ne semble toutefois pas contraire aux objectifs de la 4ème directive LCB-FT et des recommandations du GAFI. Plus généralement, les exigences françaises en

[7] La liste des moyens d'identification électronique notifiée à la Commission Européenne est accessible au lien suivant : https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

matière de vérification d'identité pour une entrée en relation à distance seraient plus contraignantes que dans les autres pays européens, plaçant les établissements français dans une situation de « concurrence inégale » face aux établissements agissant sous le régime de la libre prestation de services. Un comparatif des différentes réglementations européennes, réalisé par le Comité Banques en lignes de l'OCBF en février 2017, figure en annexe.

Si la référence au règlement eIDAS renvoie à un cadre juridique de niveau européen et favorise le développement des identités électroniques et des services de confiance dans un cadre sécurisé, fiable et interopérable, les deux nouvelles mesures de vigilance complémentaires apportées par le décret du 18 avril 2018 sont en réalité peu ou pas accessibles (à ce jour) :

- **À propos de la cinquième mesure, le moyen d'identification avec un niveau de garantie substantiel[8] :** il existe deux projets privés qui visent un niveau de garantie substantiel: (i) Mobile Connect et moi (pour les abonnés d'Orange détenteurs d'un titre d'identité français, recours à la technologie d'Ariadnext, ouverture envisagée aux abonnées Bouygues et SFR) et (ii) l'identité numérique de la Poste (qui demanderait un face-à-face préalable avec le facteur, accessible à tout détenteur d'un titre d'identité français). Une pré-notification est attendue d'ici fin 2019 à la Commission Européenne, étant noté que la notification ne peut intervenir qu'après revue par les pairs et avis du réseau de coopération ce qui prendrait au moins 6 mois. Dans ces conditions, certains membres du groupe de travail se demandent si les autorités accepteraient ces moyens d'identification dès lors que ceux-ci sont pré-notifiés à la Commission Européenne. En tout état de cause, ces deux moyens d'identification font partie de l'écosystème des fournisseurs d'identité accessibles via la plateforme France Connect[9]. Cette dernière est désormais accessible aux établissements financiers puisque ceux-ci répondent aux conditions définies dans l'arrêté du 8 novembre 2018[10]. Par-delà ces questions de qualification et de calendrier, l'utilisation effective de ces moyens d'identification par les établissements financiers dépendra aussi de plusieurs autres facteurs (coût d'utilisation, diffusion et couverture de ces moyens d'identification, incidences sur le parcours client).

- **À propos de la sixième mesure, le recueil d'une signature/d'un cachet électronique avancé(e) ou qualifié(e) reposant sur un certificat qualifié :** ces certificats sont délivrés par des prestataires de services de certification électronique qualifiés, dont les processus de vérification d'identité répondent à des exigences de sécurité et font l'objet d'un audit par un tiers organisme d'évaluation de la conformité accrédité par l'ANSSI. Certains de ces

[8] Le référentiel de l'ANSSI des exigences de sécurité applicables aux moyens d'identification électronique devrait être prochainement publié, dans la mesure où la CNIL a récemment revu le document en version de travail.

[9] Pour sécuriser ces services, la plateforme France Connect demande validation des données d'identité de l'utilisateur à l'INSEE (base Etat-civil). Il existerait des équivalents à France Connect au Royaume-Uni (GOV.UK verify), en Italie (SPID – *Sistema Pubblico di Identità Digitale* avec les trois niveaux de garantie d'eIDAS) et en Belgique (un seul fournisseur d'identité). Cf. le panorama de la Fédération bancaire européenne accessible via cette synthèse.

[10] Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'État

prestataires, dont la liste est accessible sur le site de l'ANSSI[11], commercialisent leurs offres. Le marché de la signature ou du cachet électronique reposant sur un certificat qualifié serait en train de se développer en lien avec les pratiques pour les marchés publics. Certains membres se demandent aussi pourquoi les autres services de confiance qualifiés encadrés par le règlement eIDAS comme l'envoi recommandé électronique qualifié ne sont pas reconnus comme mesure de vigilance complémentaire.

Par conséquent, certains estiment que le contenu des mesures de vigilance complémentaires a en réalité peu évolué depuis 10 ans :

- **La première mesure demande copie du document d'identité ainsi qu'un document justificatif supplémentaire.** Les lignes directrices de l'ACPR[12] indiquent que ce document doit contenir les informations confirmatives en matière d'identification du client (nom, prénom, date et lieu de naissance pour une personne physique). Cela peut être un avis d'imposition, une carte vitale, une fiche de paie ou un livret de famille. En revanche, le justificatif de domicile ne remplit pas les conditions. Cette mesure est aujourd'hui largement utilisée par les établissements financiers, alors même que cela implique la communication non sécurisée de données sensibles d'identité.
- **La seconde porte sur la mise en œuvre des mesures de vérification et de certification de la copie du document d'identité (pour une personne physique) ou d'un extrait de registre officiel (pour une personne morale) par un tiers indépendant de la personne à identifier.** La mise à jour des lignes directrices de l'ACPR a permis une ouverture sous conditions aux nouveaux prestataires technologiques privés («*Les organismes pourraient recourir à un tiers indépendant proposant des solutions technologiques dites de « vérification/certification » des copies des documents d'identité reposant, par exemple, sur des données biométriques, si ces solutions sont encadrées par un texte ou par des normes garantissant leur fiabilité et leur sécurité* »). Toutefois, aucune « *norme garantissant la fiabilité et la sécurité* » des dispositifs n'a été adoptée à ce jour. Cette seconde mesure est pour l'instant peu utilisée par les établissements financiers.
- **La troisième mesure exige que le premier paiement soit effectué en provenance ou à destination d'un compte ouvert au nom du client.** Cette mesure est largement utilisée par les établissements financiers, mais elle n'est pas ouverte aux clients qui ouvrent un compte pour la première fois.
- **La quatrième mesure consiste en l'obtention d'une confirmation de l'identité du client par un tiers lui-même assujetti à la LCB-FT.** Cette mesure est souvent utilisée entre les entités d'un même groupe financier. Elle est revanche peu accessible pour les nouveaux entrants ou les établissements de petite et moyenne taille.

Ces exigences réglementaires s'appliquent uniformément aux personnes assujetties aux obligations de LCB-FT (liste donnée par le L. 561-2 du CMF) et bientôt aux acteurs effectuant des activités liées aux crypto-actifs et couverts par la loi Pacte. Dans l'hypothèse où ce groupe de travail

[11] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

[12] Lignes directrices de l'ACPR relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, décembre 2018

venait à proposer de nouvelles mesures de vérification d'identité plus appropriées aux contraintes des organismes financiers, certains membres du groupe de travail se demandent si une différenciation entre les organismes financiers d'une part et les autres personnes assujetties à la LCB-FT d'autre part (opérateurs de jeux, commerce d'antiquités et d'œuvre d'art, les avocats etc.) ne serait pas nécessaire pour en faciliter l'introduction.

II. Proposition de solutions pour améliorer la vérification d'identité à distance

A. Acceptation d'un moyen d'identification électronique de niveau substantiel comme un équivalent au face-à-face

La réglementation a pour vocation de définir un socle commun d'exigences que chaque personne assujettie aux obligations de lutte contre le blanchiment et le financement du terrorisme (LCB-FT) doit effectuer pour vérifier l'identité de son client. Si les établissements financiers constituent la majorité des personnes concernées, la typologie des personnes assujetties aux obligations de LCB-FT est en effet extrêmement variée (L. 561-2 du code monétaire et financier).

On distingue deux grandes catégories de fraude pour les vérifications d'identité de personnes physiques[13] : l'usurpation d'identité où la personne utilise les documents d'identité authentique d'une autre personne et la fraude documentaire où la personne présente de faux documents d'identité.

Face à cette diversité, les établissements peuvent compléter ce socle commun par la mise en œuvre d'autres mesures destinées à lutter contre la fraude, selon une approche par les risques[14]. Il est également souligné que la vérification d'identité à l'entrée en relation d'affaires est une étape préalable à l'émission de moyens d'authentification qui serviront tout au long de la relation commerciale (connexion à l'espace en ligne, utilisation des moyens de paiement, souscription à de nouveaux produits etc.).

L'entrée en relation n'est pas l'unique composante de la lutte contre la fraude. . D'autres réglementations peuvent compléter les obligations de LCB-FT comme par exemple les exigences d'authentification forte et de communication sécurisée issues de la 2nde directive européenne sur les services de paiement (DSP2). Pour les établissements financiers, il y a un continuum entre les mesures de vérification d'identité mises en œuvre à l'entrée en relation et les mesures d'authentification réalisées tout au long de la relation commerciale.

Des échanges ont porté sur l'opportunité de retenir les photos des clients entrés en relation. Selon les membres du groupe, cette pratique ne serait pas jugée conforme par la CNIL. De fait, sur les

[13] Dans ce contexte, une expérimentation est en cours avec quelques établissements de la Place pour l'utilisation du traitement « DOCVERIF » qui permettrait de renforcer la lutte contre la fraude documentaire et l'usurpation d'identité en facilitant le contrôle de la validité des cartes nationales d'identité, des passeports et des titres de séjours.

[14] La lutte contre la fraude doit naturellement être distinguée de la LCB-FT et des règles qui régissent celles-ci. Néanmoins, lutte contre la fraude et LCB-FT se renforcent mutuellement.

solutions d'identification électroniques évoquées visant un niveau substantiel, la photo n'est pas automatiquement détenue par l'établissement financier ou n'est pas nécessaire pour réaliser l'identification du client (identité numérique de La Poste via un face à face physique). Pour autant, TRACFIN indique qu'elle lui est nécessaire pour certains de ses processus d'investigation.

Les moyens d'identification électronique qui obtiennent un niveau de qualification substantiel « eIDAS » pourraient compléter les mesures admises comme équivalentes au face-à-face

Les modalités de vérification d'identité électronique qui n'appellent pas de mesure de vigilance complémentaire (« équivalents au face-à-face» d'un point de vue réglementaire), qui sont listées aux 1° et 2° de l'article R. 561-5-1 du code monétaire et financier, ne sont pas accessibles aux établissements financiers. Il y a une inaccessibilité de fait : le coût de développement et de gestion des moyens d'identification électronique de niveau élevé suppose un modèle économique qui semble trop éloigné des besoins et des stratégies des établissements financiers. Par ailleurs, des contraintes juridiques fortes encadrent l'accès aux puces contenues dans les documents d'identité, dont la lecture est généralement nécessaire pour les moyens d'identification électronique de niveau élevé. À titre d'exemple, le projet d'ALICEM porté par l'ANTS qui accède et lit la puce du passeport biométrique.

Il apparaît finalement que les moyens d'identification électronique de niveau élevé correspondent à des modèles qui ne peuvent être développés que par la puissance publique.

C'est d'ailleurs l'objectif de la mission interministérielle de Mme Valérie Peneau que de développer un moyen d'identification électronique de niveau élevé (généralement résumé par le terme « identité numérique »). Compte tenu du temps de déploiement des moyens d'identification électronique de niveau élevé par la puissance publique, les établissements financiers ne disposeraient d'aucun équivalent réglementaire au face-à-face à court et moyen terme (env. 5 ans).

Les moyens d'identification électronique de niveau élevé appellent généralement des procédures de vérification d'identité qui ne peuvent être mises en œuvre que par des autorités publiques ou des personnes spécialisées dans la vérification d'identité. À contrario, les moyens d'identification électronique de niveau faible reposent sur une présomption d'identité : la personne est « présumée en possession d'un élément d'identification », qui est « présumé authentique » et qui « semble être valide » et « on peut présumer que la personne est bien celle qu'elle prétend être ».

En revanche, les moyens d'identification électronique de niveau substantiel, lorsque l'inscription se fait à distance, appellent des mesures de vérification d'identité permettant de vérifier l'authenticité du document d'identité et de s'assurer que ce document se rapporte à la personne qui le présente.

Les experts du groupe de travail reconnaissent pour la plupart que le risque de fraude est susceptible d'être plus élevé pour les entrées en relation à distance. Les entrées en relation en agence sont également soumises au risque de fraude (usurpation d'identité et fraude identitaire), mais les entrées en relation en ligne (mobile, web etc.) seraient en réalité exposées à de plus nombreuses tentatives de fraude. Il est en effet plus facile de répéter, parfois à grande échelle, des schémas de fraude auprès de différents sites en ligne ou applications mobiles qu'en se rendant dans différentes

agences (avec les aléas liés au niveau de vigilance de l'agent de l'établissement financier). Les organismes financiers devraient être en mesure de disposer de statistiques sur la fraude plus précises et plus fines, notamment en distinguant par canaux de distribution.

L'ANSSI estime toutefois que le risque de fraude plus élevé pour les procédures en ligne est pris en compte par les moyens d'identification électronique de niveau substantiel. Ainsi, la vérification d'identité embarquée dans un moyen d'identification électronique de niveau substantiel apporterait un niveau de sécurité équivalent à la vérification d'identité effectuée par un agent d'établissement financier en agence.

Proposition n°1

Au même titre que les moyens d'identification électronique de niveau élevé, considérer que le recours à un moyen d'identification électronique de niveau substantiel réponde aux obligations de vérification d'identité des établissements financiers sans appeler aucune mesure de vigilance complémentaire. Le recours à un moyen d'identification électronique de niveau substantiel serait l'une des modalités listées au R. 561-5-1 du code monétaire et financier et ne serait en conséquence plus listé parmi les mesures de vigilance complémentaires du R. 561-20.

Considérant qu'une entrée à relation à distance est porteuse d'un risque accru en matière de fraude et usurpation d'identité, TRACFIN estime que les solutions en cours de développement sur l'identité numérique devraient pouvoir apporter une confiance encore plus importante que lors d'une relation en face à face. C'est pourquoi TRACFIN défend la réglementation existante qui permet l'entrée en relation sans mise en œuvre de mesures de vigilance complémentaires si l'identification du client est de niveau élevé au sens du règlement eIDAS. Sa préférence se porte donc sur une identité numérique publique telle que développée par le programme ALICEM qui offre davantage de garantie, en particulier au titre de la collecte du renseignement en matière de lutte contre le financement du terrorisme. TRACFIN considère également que le manque de recul sur la viabilité des moyens techniques de vérification d'identité relevant du niveau substantiel, ne lui permet pas, à ce stade, de soutenir la proposition du groupe de travail. C'est pourquoi TRACFIN souhaite évoquer rapidement avec l'ACPR et l'ANSSI les modalités concrètes de l'évaluation de la conformité des dispositifs de niveau substantiel afin de s'assurer que les différents risques en matière LCB/FT sont bien pris en compte.

B. Un nouveau référentiel de place pour évaluer de nouvelles modalités de vérification d'identité en mesure de vigilance complémentaire

Pour rappel, le groupe de travail estime que les établissements financiers pourront à moyen terme disposer de plusieurs moyens d'identification électronique de niveau substantiel, certains d'entre eux étant accessibles via la plateforme *France Connect*. Toutefois, la qualification comme moyen d'identification électronique de niveau substantiel par des acteurs privés suppose la définition d'un modèle économique.

Or, si cette réflexion stratégique peut exister pour amortir les coûts engagés au titre de la LCB-FT, la majorité des établissements financiers ne souhaitent pas devenir des fournisseurs d'identité. Ils travaillent en revanche avec des prestataires technologiques spécialisés pour améliorer leurs modalités de vérification d'identité au regard des objectifs de LCB-FT, lutte contre la fraude et d'amélioration du parcours client. Ces nouvelles modalités de vérification d'identité n'ont pas forcément pour objet d'être offertes à des acteurs extérieurs.

Dans ces conditions, l'obtention par les établissements financiers d'une qualification comme moyen d'identification électronique de niveau substantiel n'a pas été une option retenue par le groupe de travail.

Vers un référentiel de place pour la vérification d'identité dans le cadre de la cinquième mesure du R. 561-20 du Code Monétaire et Financier

Le référentiel d'exigences de sécurité sur les moyens d'identification électronique de l'ANSSI, qui vient préciser les exigences du règlement d'exécution européen[15] montre que la qualification comme moyen d'identification électronique demande de respecter des exigences qui vont au-delà de la seule vérification d'identité. Or, c'est la brique « vérification d'identité », comprise dans le chapitre des exigences portant sur l'inscription, qui est recherchée dans la définition du « socle commun » réglementaire en matière d'entrée en relation. En revanche, les chapitres des exigences portant sur la gestion des moyens d'identification électronique, l'authentification ou la gestion et l'organisation ne portent pas spécifiquement sur la vérification d'identité et semblent contingents pour répondre aux besoins des établissements financiers.

Un nouveau référentiel, inspiré de la partie du référentiel de l'ANSSI portant sur la vérification d'identité, pourrait constituer le socle d'une nouvelle mesure de vigilance complémentaire pour les objectifs d'identification et de vérification (R. 561-20) pour remplacer la cinquième mesure actuellement en vigueur. Les modalités de vérification d'identité qui seraient jugées au moins équivalentes au niveau de sécurité substantiel ne seraient toutefois pas jugées équivalentes à l'entrée en relation en face à face (R. 561-5-1), car l'évaluation ne porterait que sur une partie du référentiel complet de l'ANSSI. La conformité à l'ensemble du référentiel reste plus exigeante (gestion des moyens d'identification dans le temps, organisation du fournisseur, sécurité informatique etc.).

Les travaux du groupe de travail montrent qu'aucun autre référentiel n'est disponible en matière de vérification d'identité. La norme ISO 29115 :2013 « Cadres d'assurance de l'authentification d'entité » en cours de révision n'étant pas jugée compatible avec la normalisation « eIDAS » par l'ANSSI. Par ailleurs, chaque établissement possède son propre cahier des charges et aucune concertation de place n'a eu lieu pour les harmoniser.

Afin que ce nouveau référentiel de vérification d'identité conserve sa pertinence au cours du temps et soit enrichi régulièrement, il doit prendre en compte les évolutions du référentiel sur les moyens d'identification électroniques de l'ANSSI. **Pour cette raison, les membres du groupe proposent de**

[15] Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés par l'article 8, paragraphe 3, du règlement (UE) n°910/2014 .

construire la nouvelle cinquième mesure avec une référence directe aux parties pertinentes du référentiel d'exigences de sécurité sur les moyens d'identification électronique de l'ANSSI. Cette solution offre les meilleures garanties d'adaptabilité du nouveau référentiel et de facilité pour son évaluation. Les échanges entre les organismes d'évaluation et l'ANSSI (cf. infra), ainsi que la mise en place d'un groupe de travail technique permettraient de faciliter la mise en œuvre du nouveau référentiel de vérification.

Les membres du groupe de travail ont également échangé à propos des documents d'identité reconnus par le référentiel sur les moyens d'identification électroniques de l'ANSSI. Bien que soient acceptés, en sus des passeports français et de l'Union Européenne, des passeports non-européens si le pays est dispensé de visa, le périmètre des documents reconnus est susceptible d'être un peu trop limité. L'absence des permis de conduire parmi les pièces d'identités acceptées par le référentiel a ainsi été relevée. L'inclusion de nouveaux documents d'identité dans le référentiel peut être étudiée mais elle implique l'accord de différentes parties, tel le Ministère de l'Intérieur, dont les objectifs peuvent faire obstacle à un élargissement trop important des pièces d'identité étrangères reconnues.

Adaptation de la première mesure de vigilance complémentaire

La modification de la cinquième mesure de vigilance complémentaire qui permet d'atteindre un niveau de sécurité important prendra tout son sens si elle permet de faciliter concrètement le parcours client. Or, la validation de cette mesure peut être réalisée lors de la même étape du parcours client que la transmission d'un document d'identité, correspondant en partie à la première mesure de vigilance complémentaire. L'utilisation conjointe de la première et de la nouvelle cinquième mesure de vigilance complémentaire constitue pour les établissements financiers une solution efficace et réalisable. Dans ce contexte, le groupe de travail a proposé, en cas d'utilisation combinée de ces deux mesures de vigilance complémentaire, de réduire les exigences de la première mesure à une seule pièce d'identité avec photo (CNI, passeport, carte de résident).

Proposition n°2.1

Établir un nouveau référentiel de place centré sur la vérification d'identité en s'inspirant du référentiel de l'ANSSI sur les moyens d'identification électronique par une référence directe aux parties pertinentes du référentiel ANSSI dans le R.561-20 modifié par décret, adaptées le cas échéant aux exigences spécifiques des acteurs financiers, notamment relatives à la LCB-FT.

Dans le cas où la première et la cinquième mesure de vigilance complémentaire seraient utilisées conjointement, seule une pièce d'identité avec photo pourrait être demandée au titre de la première mesure.

Modalités d'évaluation du nouveau référentiel pour la cinquième mesure du R. 561-20

Une fois le référentiel décidé, il reste à définir ses modalités d'évaluation à la fois au moment de la mise en place d'une nouvelle modalité de vérification d'identité et dans la durée pour vérifier que son niveau de sécurité reste suffisant. Trois options ont été débattues par les membres du groupe de travail :

(i) Évaluation par une autorité publique

Cette solution aurait l'avantage d'assurer une évaluation cohérente des différents dispositifs de vérification d'identité, mais la procédure d'évaluation pourrait ne pas être aussi rapide que souhaitée[16]. En conséquence, elle n'a pas été retenue par les membres du groupe de travail.

(ii) Évaluation par des organismes d'évaluation indépendants certifiés par une autorité publique

En recourant aux organismes d'évaluation de la conformité des prestataires de services de confiance reconnus par l'ANSSI, cette solution permettrait un calendrier flexible et une accessibilité à l'ensemble des acteurs.

(iii) Évaluation par le dispositif de contrôle interne des établissements financiers

En complément de l'évaluation par des organismes indépendants, certains établissements bancaires souhaiteraient internaliser l'évaluation[17]. Cette option a été rejetée car, outre le fait qu'aucun critère d'évaluation n'a été proposé, l'ANSSI ne semble pas favorable à certifier des banques pour leur capacité à s'autoévaluer.

La solution préférée par le groupe de travail est donc l'évaluation par des prestataires de services de confiance qualifiés certifiés par l'ANSSI. Elle permet de développer un écosystème d'évaluation pour s'assurer de la conformité des établissements financiers au référentiel de la cinquième mesure[18]. Pour être pleinement efficace, il faudra qu'une fois la règlementation modifiée, un nombre suffisant de prestataires soient certifiés dans un délai réduit.

À cet égard, l'ANSSI a appelé l'attention du groupe de travail sur le fait que la mise en place d'un tel écosystème prendrait du temps. L'option d'une évaluation par des prestataires de service certifiés ne lui paraît pas viable à court terme, même s'il peut s'agir d'un objectif à atteindre. L'ANSSI propose donc d'évaluer directement les solutions selon l'option (i) exposée *supra*, une migration vers l'option (ii) pouvant être réalisée dans un second temps, quand l'écosystème aura gagné en maturité.

Renouvellement des certifications et contrôles

Le groupe de travail propose une fréquence de revue de l'évaluation au maximum tous les 2 ans, afin de conserver la même périodicité que celle en vigueur pour l'identification électronique de niveau substantiel eIDAS.

En revanche, il n'a pas été jugé adapté de définir une fréquence d'autoévaluation. Le contrôle permanent des établissements financiers requiert une adéquation permanente de la conformité du dispositif de LCB-FT, réduisant la pertinence d'imposer une fréquence arbitraire pour

[16] L'ANSSI indique avoir besoin d'au moins 2 mois incompressibles d'accès au système évalué, en coopération avec la gendarmerie nationale, induisant des délais organisationnels supplémentaires, tandis que l'évaluation par des organismes d'évaluation indépendants efficaces et en nombre suffisant pourrait raccourcir les durées d'évaluations.

[17] Les Fintechs et autres établissements de petite taille ne disposent généralement pas d'un département d'audit à même de s'autoévaluer.

[18] La validation d'un cas type de solution ne pourra pas être répliquée, le risque évalué se matérialisant généralement dans l'implémentation de la méthode de la solution.

l'autoévaluation du dispositif[19]. En outre, la modification de paramètres réalisée dans le cadre de la certification devra être tracée par l'établissement et un rapport d'activité adapté sur les niveaux de fraude constatés mis en place.

Proposition n°2.2

Faire évaluer la conformité des solutions des établissements vis-à-vis du référentiel proposé en 2.1 par des organismes d'évaluation indépendants certifiés par l'ANSSI. Prévoir toutefois un dispositif transitoire où l'ANSSI effectuerait elle-même cette évaluation.

La période entre chaque évaluation réalisée sera d'au maximum deux ans et les établissements devront s'assurer en continu de l'efficacité de leur dispositif, conformément à la règlementation sur le contrôle interne en vigueur.

C. Extension du périmètre de la sixième mesure de vigilance complémentaire à l'envoi de recommandé électronique

Les services de confiance (signature électronique ou cachet électronique) reposant sur un certificat qualifié comportent également une « brique » de vérification d'identité.

En effet, l'article 24 du règlement (UE) 910/2014 eIDAS dispose que « *lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié* ». Cette vérification d'identité peut être effectuée (i) par un contrôle en face-à-face, (ii) par le recours à un moyen d'identification de niveau substantiel ou élevé ou (iii) « *à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne* », l'équivalence étant confirmée par un organisme d'évaluation de la conformité[20].

Ainsi, un service de confiance encadré par le règlement (UE) 910/2014 eIDAS comportant la délivrance d'un certificat qualifié qui permet de vérifier l'identité du client entrant en relation peut constituer une mesure de vérification complémentaire. L'envoi de recommandé électronique qualifié (art. 44 du règlement eIDAS), rentre dans cette catégorie. En revanche, l'horodatage électronique ne permet pas d'identifier le client via le certificat qualifié car la signature/cachet électronique requise par l'article 42 du règlement eIDAS est celle de la personne morale ou physique qui opère le service d'horodatage mais pas celle du client souhaitant entrer en relation.

Le recueil d'un service de confiance reposant sur un certificat qualifié ne permet pas à l'établissement de vérifier tous les éléments d'identification normalement requis pour l'identification

[19] L'ACPR a par ailleurs rappelé que les potentielles défaillances doivent dans tous les cas être résolues dès leur constat par les entités assujetties.

[20] La liste des organismes d'évaluation de conformité est publiée sur le site de l'ANSSI : https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/centres-evaluation/

d'une personne physique en face-à-face (R. 561-5-1). Les nom et prénoms sont vérifiables mais pas la date et le lieu de naissance, contrairement à un document officiel en cours de validité permettant d'obtenir toutes ces informations. Pour ces raisons, le maintien dans la catégorie des mesures de vigilance complémentaire (R. 561-20) des services de confiance reposant sur un certificat qualifié (signature/cachet électronique) semble nécessaire.

Proposition n°3

Inclure dans la réglementation, outre la signature électronique et le cachet électronique, l'envoi de recommandé électronique au sein de la sixième mesure de vigilance complémentaire de l'article R. 561-20 du CMF regroupant les services de confiance reposant sur un certificat qualifié offrant les mêmes garanties de vérification.

D. Mettre en place un *reporting* mesurant l'efficacité du dispositif

Les propositions précédentes, notamment portant sur la modification des cinquième et sixième mesures complémentaires décrites dans le R. 561-20 du code monétaire et financier, devraient être accompagnées d'une mesure minimale de l'efficacité du dispositif pour permettre aux établissements de contrôler en continu le niveau de sécurité de leur dispositif de vérification d'identité à distance.

Les membres ont souligné l'importance de permettre une future auditabilité par les services d'audit des établissements et le cas échéant des autorités de supervision compétentes (ACPR et AMF). Des échanges devront toutefois avoir lieu selon le type de solution technique adoptée et prendre en compte la contrainte opérationnelle des établissements financiers.

Proposition n°4

À l'image de ce qui est réalisé en matière de fraude sur les moyens de paiement par la Banque de France, établir une nouvelle obligation de *reporting* pour permettre d'apprécier la qualité et l'efficacité des différentes procédures d'entrée en relation (à distance et face-à-face) . Le modèle, la fréquence et les délais de transmission de ce *reporting* pourront faire l'objet de discussions ultérieures.

Ce *reporting* aurait pour objectif de s'assurer de l'efficacité du dispositif et d'envisager, le cas échéant, des modifications de la réglementation par les autorités publiques lorsque d'autres moyens d'identification seront disponibles.

Par ailleurs, à l'occasion des travaux mais indépendamment des propositions ci-dessus, le groupe de travail a noté que les mesures de vérification d'identité seront progressivement moins « documentaires » (par exemple identification via France Connect si cette plateforme embarque un moyen d'identification électronique de niveau substantiel) : il conviendra de s'interroger sur la faisabilité technique de la piste d'audit pour les moyens d'identification électronique (conservation des « traces » numériques).

E. Simplifier la réglementation sur l'entrée en relation

En matière de vérification d'identité, l'article R312-2[21] du Code monétaire et financier, impose au « banquier » - les autres établissements teneurs de compte comme les établissements de paiement ou les établissements de monnaie électronique ne sont a priori pas concernés - de vérifier le domicile et l'identité du postulant préalablement à l'ouverture du compte. En l'absence d'alternative, cette diligence supplémentaire conduit beaucoup d'établissements de crédit à demander un justificatif de domicile avant l'ouverture du compte à des fins de vérification de domicile.

Cette disposition n'est pas liée à la lutte contre le blanchiment et le financement du terrorisme. En la matière, une disposition proche mais distincte figure dans le code général des impôts (article 1649 AC) : elle impose l'identification de la résidence fiscale sans pour autant qu'un justificatif de domicile ne soit requis.

Aussi convient-il de s'interroger sur les avantages à conserver à cet usage le caractère d'une exigence réglementaire, susceptible d'alourdir le processus d'entrée en relation à distance[22].

Afin de simplifier le cadre règlementaire et d'en améliorer la lisibilité, les membres du groupe de travail s'interrogent sur l'opportunité de supprimer l'article R.312-2 du code monétaire et financier

Naturellement, le justificatif de domicile pourra continuer à être demandé, avant ou après l'ouverture du compte, par les établissements dans le cadre de leur politique interne, au titre de la LCB-FT (arrêté du 2 septembre 2009 pris en application de l'article R.561-12 du code monétaire et financier) ou de la lutte contre la fraude.

Proposition n°5

Inviter la DG Trésor à évaluer la nécessité de conserver l'article R312-2 du Code monétaire et financier, afin de le supprimer le cas échéant.

[21] « *Le banquier doit, préalablement à l'ouverture d'un compte, vérifier le domicile et l'identité du postulant, qui est tenu de présenter un document officiel comportant sa photographie. Le banquier doit recueillir et conserver les informations suivantes : nom, prénoms, date et lieu de naissance du postulant, nature, date et lieu de délivrance du document présenté et nom de l'autorité ou de la personne qui l'a délivré ou authentifié.*

Pour l'ouverture d'un compte au nom d'une personne morale, le banquier demande la présentation de l'original ou l'expédition ou la copie de tout acte ou extrait de registre officiel datant de moins de trois mois constatant la dénomination, la forme juridique, l'adresse du siège social et l'identité des dirigeants.

Pour l'application des dispositions du premier alinéa, l'adresse du centre communal ou intercommunal d'action sociale ou de l'organisme agréé au titre de l'article L. 264-2 du code de l'action sociale et des familles figurant sur la carte nationale d'identité en application des dispositions du cinquième alinéa de l'article 2 du décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité vaut justification du domicile. Il en est de même de l'attestation d'élection de domicile présentée par la personne ne disposant pas d'un domicile stable instituée par le même article. »

[22] Ces avantages pourraient découler d'éventuelles références à cet article, que le groupe de travail n'a pas eu la possibilité d'identifier dans le temps imparti.

Annexe I - Liste des membres du groupe de travail

Organisme	Représentant
ACPR - Agent de liaison TRACFIN	Laurent Clerc
ACPR - Direction des affaires juridiques	Yvan Bazouni
ACPR - Direction des affaires juridiques	Emmanuelle Boucher
ACPR - Direction des affaires juridiques	Alois Gareste
ACPR - Direction des agréments	Geoffroy Goffinet
ACPR - Direction des agréments	Jonathan Hongrois
ACPR - Direction du contrôle bancaire	Jean-Gaspard d'Ailhaud de Brisis
ACPR - Direction du contrôle bancaire	Philippe Ruez
ACPR - Direction du contrôle bancaire	Sofiène Moumen
ACPR - Pôle Fintech-Innovation	Olivier Fliche
ACPR - Pôle Fintech-Innovation	Pierre Bienvenu
ACPR - Pôle Fintech-Innovation	Arthur Moraglia
AMF - Direction juridique	Patricia Choquet
AMF - Direction juridique	Anne-Laure Bardou
AMF - Division Fintech-Innovation	Alexandre Barrat
ANSSI	Romain Santini
ANSSI	Lisa Allemand
ANSSI	Grégoire Lundi
Ariadnext	Guillaume Despagne
ASF	Corinne Denaeyer
BforBank	Sébastien Golfier
BNPP	Olivier Van Den Bilcke
BPI	Julien Belhassen
Circle	Daniel Benamran
CNIL	Clémence Scottez
CNIL	Flora Plénacoste
DGT - BANCFIN4	Arnaud Delaunay
DGT - BANCFIN4	Clément Robert
DGT - MULTICOM	Arjoun Raj
DGT - MULTICOM	Eleonore Peyrat
DGT - PAESF	Yannis Kemel
FBF	Frédérique Fages
FBF	Judith Azevedo
Fortunéo	Rozenn Le Rhun
France Connect	Lionel Fouillen
France Connect	Stephane Mavel
ID-Now	Typhaine Gaudemer
Lydia	Alison Alonso
Morpho	Philippe Le Pape
Netheos	Olivier Détour
OCBF	Anne-Marie Moulin
OCBF	Camille Montet

OCBF	Carole d'Armaillé
Onfido	Gimena Diaz
Orange Bank	Anne-Sophie Duquennoy
Qonto	Jean-Eloi Rateau
TRACFIN	Cyprien Scherrer
TRACFIN	Jocelyn Lelong
Ubble	Juliette Delanoe

1. L'écosystème de l'identité numérique et le monde bancaire : panorama des systèmes d'identité numérique à l'international *(date : 19/03/2019)*

CRITERES	Royaume-Uni	Belgique	Allemagne	Italie
Schéma d'identification électronique notifié	*Government eID scheme (GOV.UK Verify)*	**Schéma belge d'identification électronique FAS / Cartes d'identité électroniques 27/12/2018**	**Schéma allemand d'identification électronique fondé sur le contrôle d'accès étendu (CNI + permis de séjour électronique) 26/09/2017**	**SPID – Système public d'identité numérique (moyens d'identification électronique fournis par des sociétés privées) 10/09/2018**
Carte d'identité électronique et/ou biométrique	non	Carte d'identité électronique pour ressortissants belges Carte d'identité électronique pour étrangers >> faible taux d'acceptation par les clients bancaires	Carte d'identité nationale et eID notifiées eiDAS >> faible taux d'acceptation par les clients bancaires	« Carta di identita electronica »
Autres moyens d'identification		E-IDs (comme l'app Itsme) >> taux d'acceptation moyen par les clients bancaires	1. Video identification >> taux d'acceptation élevé 2, Qualified electronic signatures (eIDAS) >> Faible taux d'acceptation	1, Signature électronique qualifiée ou avancée >> taux d'acceptation moyen
Registre national des personnes	non	Oui	Oui	?
Identité numérique « publique »		Oui (niveau élevé)	Oui (niveau élevé)	Oui (niveaux : élevé, substantiel, faible)
Identité numérique « privée »	Oui (niveau substantiel)	Oui (ItsMe)	Oui (initiative en parallèle)	Oui (implication des sociétés privées dans la solution notifiée)
Consortium privé	Liste de sociétés certifiées (Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail, SecureIdentity)	Belgian Mobile ID (telcos et banques)	Verimi (banques, assurances, telcos…)	Liste de sociétés privés (Aruba, Namirial, InfoCert, In.TeS.A., Poste Italiane, Register.it, Sielte, Telecom Italia Trust Technologies)
Accès aux services publics en ligne : e-administration, signature de documents administratifs, vote en ligne…	Accès à GOV.UK	Interopérabilité privé/publique depuis 2018	Oui	Oui
Extension aux services privés : banques, telcos, e-commerce, jeux en ligne…	Pas d'utilisation privée	Oui		Oui

1. L'écosystème de l'identité numérique et le monde bancaire : panorama des systèmes d'identité numérique à l'international

CRITERES	Croatie	Espagne	Estonie	Luxembourg
Schéma d'identification électronique notifié	**Système national d'identification et d'authentification (NIAS) 07/11/2018**	**Documento Nacional de Identidad electronico (DNIe) 07/11/2018**	**Schéma estonien d'identification électronique : ID card, RP card, Digi-ID, eResidency Digi-ID, Mobiil-ID, carte d'identité diplomatique 07/11/2018**	**Carte nationale d'identité luxembourgeoise (eID) 07/11/2018**
Carte d'identité électronique et/ou biométrique	Carte d'identité personnelle (eOI)	Carte d'identité nationale (DNIe)	Carte d'identité, carte de séjour, carte d'identité numérique , carte numérique de résidence électronique, identification par téléphone portable, carte d'identité diplomatique	Carte nationale d'identité luxembourgeoise (eID)
Autres moyens d'identification		1. Identification vidéo (sans interlocuteur) 2. « Video call » 3. Signature électronique qualifiée (eIDAS) >> taux d'acceptation élevé		
Registre national des personnes			**Oui**	
Identité numérique « publique »	Oui (niveau élevé)	Oui (niveau élevé)	Oui (niveau élevé)	Oui (niveau élevé)
Identité numérique « privée »			Oui	
Consortium privé			Tous secteurs	
Accès aux services publics en ligne : e-administration, signature de documents administratifs, vote en ligne…			Oui	
Extension aux services privés : banques, telcos, e-commerce, jeux en ligne…			Oui (payant hors usage occasionnel)	

1. L'écosystème de l'identité numérique et le monde bancaire : panorama des systèmes d'identité numérique à l'international

CRITERES	Portugal	Autriche	République tchèque	Danemark
Schéma d'identification électronique notifié	Cartao de cidadao 28/02/2019			*Probablement en 2020 avec une nouvelle solution*
Carte d'identité électronique et/ou biométrique	Carte nationale d'identité portugaise (eID)	eID Austrian citizen card et eIDs notifiés eIDAS remplissant certains critères >>Faible taux d'acceptation		National eID
Autres moyens d'identification		1. Video identification >> taux d'acceptation moyen 2, Qualified electronic signatures (eIDAS) >>Faible taux d'acceptation	Enrôlement à distance fondé sur la vérification de l'identité du client par un prestataire de service de confiance qualifié >> taux d'acceptation moyen	Enrôlement à distance fondé sur l'identité nationale électronique, complétée par un scan de la carte d'assurance santé nationale, d'un passeport ou d'un permis de conduire >> taux d'acceptation élevé
Registre national des personnes				
Identité numérique « publique »	Oui (niveau élevé)			
Identité numérique « privée »				
Consortium privé				
Accès aux services publics en ligne : e-administration, signature de documents administratifs, vote en ligne…				
Extension aux services privés : banques, telcos, e-commerce, jeux en ligne…				

1. L'écosystème de l'identité numérique et le monde bancaire : panorama des systèmes d'identité numérique à l'international

CRITERES	Pays-Bas	Roumanie	Slovaquie	Lettonie
Schéma d'identification électronique notifié	*Pas d'eID nationale*			
Carte d'identité électronique et/ou biométrique			Discussion en cours concernant l'utilisation de la carte d'identité nationale pour l'enrôlement client	
Autres moyens d'identification	1. Scan du passeport + photo >> Taux d'acceptation moyen 2. Lecture des données du passeport >> Taux d'acceptation moyen 3. Identification vidéo >> Taux d'acceptation moyen	Identification vidéo (utilisant les documents d'identité traditionnels)	1. Enrôlement client à distance (fondé sur le scan de la carte d'identité nationale et un second document) + virement ou vérification en face à face (courrier) >> taux d'acceptation moyen 2. Moyens d'identification biométriques (équivalence d'un face-à-face physique >> taux d'acceptation moyen	1. Identification vidéo >> taux d'acceptation moyen 2. Identification avec une signature électronique sécurisée ou une solution e-ID (solution opérée par la Radio et Télévision d'Etat, solutions bancaires…) >> taux d'acceptation élevé 3. Solutions basées sur l'acquisition de données d'une institution de crédit ou de paiement, sur une reconnaissance faciale
Registre national des personnes				
Identité numérique « publique »				
Identité numérique « privée »				
Consortium privé	IDIN – eID créée par les banques >> taux d'acceptation moyen			
Accès aux services publics en ligne : e-administration, signature de documents administratifs, vote en ligne…				
Extension aux services privés : banques, telcos, e-commerce, jeux en ligne…				

1. L'écosystème de l'identité numérique et le monde bancaire : panorama des systèmes d'identité numérique à l'international

CRITERES	Grèce	Hongrie	Irlande	Suède
Schéma d'identification électronique notifié			*Pas d' ID scheme national*	
Carte d'identité électronique et/ou biométrique	Nouvelle carte d'identité biométrique (empreintes, reconnaissance faciale…) >> en cours de déploiement jusqu'en 2020			
Autres moyens d'identification	1. Signature électronique qualifiée ou avancée >> taux d'acceptation fort (entreprises) >> taux d'acceptation faible (client) 2. Solutions innovantes dans le processus de KYC fondées sur l'identification vidéo, la biométrie via les différents canaux >> en attente d'adoption par la Banque de Grèce au 1er semestre 2019	Identification vidéo >> taux d'acceptation moyen	Enrôlement video (certaines banques pour certains clients)	1. Identités électroniques (eIDAS) >> pas utilisé 2. Signature électronique qualifiée >> pas utilisé
Registre national des personnes				
Identité numérique « publique »				
Identité numérique « privée »				BankID - Solution d'identité électronique des banques suédoises >> « 100 % du marché »
Consortium privé			*Travaux préparatoires pour un ID scheme bancaire*	
Accès aux services publics en ligne : e-administration, signature de documents administratifs, vote en ligne…				
Extension aux services privés : banques, telcos, e-commerce, jeux en ligne…				

Annexe III – Benchmark sur l'identification à distance en Europe (Office de Coordination Bancaire et Financière)

Benchmark – Entrée en relation
Comité des Banques en ligne

10 février 2017

Dans le cadre de la transposition en droit français de la quatrième directive anti-blanchiment, le Comité des Banques en ligne de l'OCBF a échangé sur les exemples concrets de dispositions adoptées par différents pays européens en matière d'identification à distance. Ces dispositions sont un enjeu majeur pour les établissements de l'OCBF afin d'évoluer dans un environnement de concurrence équitable.

Vous trouverez ci-joint un benchmark de la situation dans certains pays européens qui ont intégré dans leurs réglementations de nouvelles technologies, ainsi que deux exemples de solutions déjà mises en œuvre par des banques. Une option qui se développe consiste, en particulier, à faire de l'utilisation de la visioconférence ou de médias assimilés un procédé d'entrée en relation équivalent au face à face. Plusieurs banques ont pu, sur cette base, adapter leurs processus d'entrée en relation à distance, améliorant ainsi significativement l'expérience client tout en préservant un niveau de sécurité élevé.

Il nous semble opportun dans ces conditions, à l'occasion de ces travaux de transposition, d'intégrer ce dispositif dans l'article R. 561-20, en cohérence avec le règlement Européen eIDAS de 2014.

ALLEMAGNE

1. Contexte réglementaire

Les directives 2005/60/CE et 2006/70/CE ont été transposées en droit allemand par une loi du 13 août 2008, entrée en vigueur le 21 août 2008 et révisée en juillet 2013 (*Geldwäschegesetz – GwG*, ci-après la « *loi anti-blanchiment allemande* »).

Selon une circulaire du ministère fédéral des finances (*Bundesministerium der Finanzen – BMF*), les mesures de vigilance renforcées prévues par la loi anti-blanchiment allemande en cas d'entrée en relation à distance ne sont pas applicables en cas de communication par visioconférence permettant un contact verbal avec le client et la vérification de son identité au moyen d'une pièce d'identité, une telle communication étant assimilée à du face à face[23].

La procédure d'identification par visioconférence est soumise aux conditions suivantes :

[23] Source : https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm_en.html

a. L'identification est effectuée par un collaborateur ayant suivi une formation appropriée ou par un sous-traitant avec lequel l'établissement a contracté dans les conditions prévues par la loi anti-blanchiment allemande.
b. Le collaborateur est situé dans un local séparé à accès réservé.
c. L'accord exprès du client est recueilli au début de la procédure.
d. Au cours de la visioconférence :
   - le client produit une pièce d'identité comportant des marques optiques permettant d'en vérifier l'authenticité ;
   - le collaborateur s'assure que la pièce d'identité est authentique et n'a pas été altérée ; il s'assure qu'elle correspond bien au client et vérifie la cohérence de la date de naissance du client, de la date d'émission de la pièce d'identité et des données d'identification recueillies en général ;
   - le collaborateur prend des photos ou des impressions d'écran du client et du recto et verso de la pièce d'identité ;
   - le client lit le numéro de la pièce d'identité ;
   - le client saisit en ligne un code à usage unique (TAN) qui lui a été envoyé par courriel ou par SMS.
e. La conversation fait l'objet d'un enregistrement audio.

ESPAGNE

1. Contexte réglementaire

La directive 2005/60/CE a été transposée en droit espagnol par la loi 10/2010 (ci-après la « *loi anti-blanchiment espagnole* ») et par le décret royal 304/2014. Ce dernier décrit, dans son article 21, les exigences en matière d'entrée en relation, notamment dans le cas où le client n'est pas présent physiquement.

L'entrée en relation ou l'exécution de transactions peuvent être réalisées par téléphone ou de manière électronique ou télématique si l'une des conditions suivantes est respectée :

a. L'identité du client est vérifiée conformément aux dispositions de la loi relative à la signature électronique.
b. L'identité du client est vérifiée par production d'une copie notariée de pièce d'identité.
c. Un premier paiement est effectué en provenance d'un compte ouvert au nom du client dans un autre établissement situé en Espagne, dans l'Union Européenne ou dans un pays tiers équivalent.
d. L'identité du client est vérifiée par l'utilisation d'un autre procédé d'identification à distance sûr, à condition que ce procédé ait été préalablement approuvé par le SEPBLAC (*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*).

Sur la base de l'article 21.1.d) de la loi anti-blanchiment espagnole, la SEPBLAC a approuvé, sous la forme d'une autorisation unique en date du 12 février 2016[24], la mise en œuvre de

[24] Source : http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf

procédures d'identification par visioconférence de clients non physiquement présents aux conditions suivantes :

a. La procédure fait l'objet d'une analyse de risque et de tests préalables documentés, ainsi que d'un rapport d'expertise externe en confirmant la pertinence et l'efficacité.
b. Préalablement à l'identification, l'établissement s'assure que le client n'a pas fait l'objet de sanctions financières ou de sanctions internationales conformément à la loi 10/2010.
c. L'identification est effectuée par un collaborateur ayant suivi une formation appropriée.
d. Des mesures sont prises pour assurer la confidentialité de la visioconférence.
e. L'accord exprès du client pour la vérification d'identité par vidéo et son enregistrement est recueilli.
f. Le client présente de façon lisible le recto et le verso d'une pièce d'identité et des photographies en sont prises et conservées ; les conditions de communication permettent de vérifier que la pièce d'identité présentée est bien authentique et intacte et qu'elle correspond bien au client.
g. Le processus d'identification est enregistré et horodaté et l'enregistrement conservé conformément aux exigences de la loi 10/2010.
h. Le processus d'identification par visioconférence peut être externalisé, mais l'établissement en reste responsable.

2. Exemples de solutions mises en œuvre

Une banque a informé la SEPBLAC de la mise en œuvre d'une nouvelle procédure d'entrée en relation par visioconférence.

Cette procédure n'utilise pas la visioconférence en temps réel mais l'enregistrement d'une séquence vidéo au cours de laquelle le client est guidé automatiquement et des photos de lui-même et de sa pièce d'identité réalisées. La séquence vidéo et la cohérence d'ensemble des données recueillies (appréciée sur plus d'une vingtaine de points) sont vérifiées a posteriori. La SEPBLAC n'ayant formulé aucune objection, cette procédure a été mise en production.

D'autres banques espagnoles utilisent déjà la visioconférence dans leur parcours d'entrée en relation avec des clients non physiquement présents

ITALIE

1. Contexte réglementaire

La directive 2005/60/CE a été transposée en droit italien par le décret législatif 231/2007 du 21 novembre 2007, complété par différents règlements d'exécution (*provvedimenti*) de la

Banca d'Italia, notamment le règlement du 11 avril 2013 relatif à l'identification de la clientèle[25].

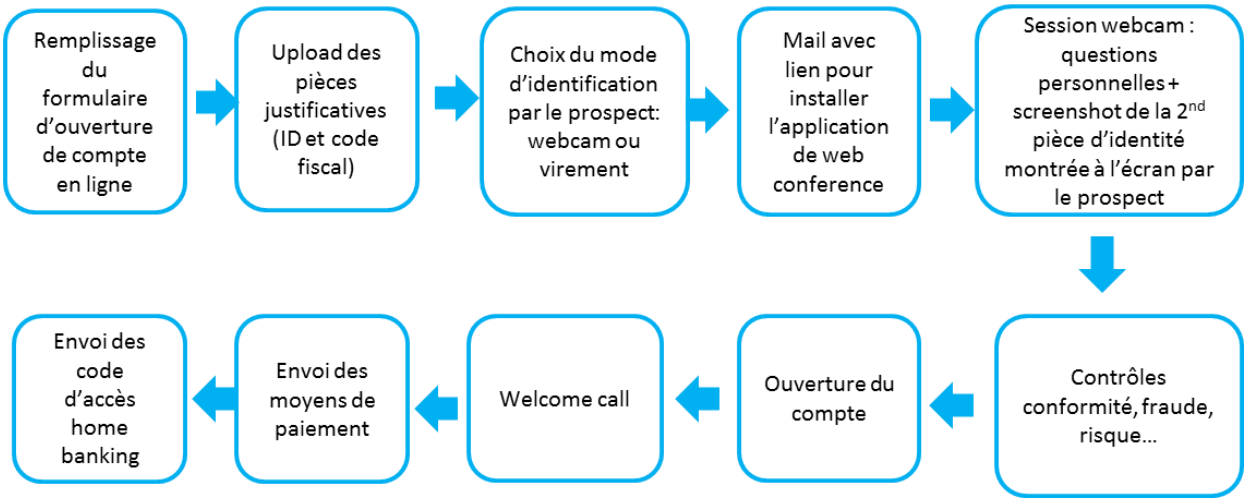
Quel que soit le mode d'entrée en relation (en face à face ou à distance), l'identification requiert la présentation par le client d'une pièce d'identité en cours de validité et la communication de son code fiscal.

L'arrêté du 3 avril 2013 mentionne expressément, parmi les modes possibles d'entrée en relation à distance, la communication par téléphone et par internet. Dans ce cas :

a. une copie de la pièce d'identité du client est transmise à l'établissement par télécopie, par courrier ou au format électronique, et les données d'identification recueillies à distance lui sont comparées ;
b. des mesures de vérification complémentaires adaptées au risque présenté sont prises (par exemple un appel de bienvenue vers un numéro de téléphone fixe ou l'envoi d'un courrier recommandé avec accusé de réception à l'adresse du client), le règlement ne listant toutefois pas de façon exhaustive les mesures susceptibles d'être mises en œuvre.

2. Exemples de solutions mises en œuvre

Sur la base de la réglementation ci-dessus, une banque française en Italie a mis en place une procédure d'identification à distance utilisant notamment la visioconférence, selon le schéma suivant :



Cette procédure a été présentée au régulateur italien avant sa mise en œuvre. Elle a depuis été également mise en œuvre par d'autres établissements.

SUISSE

[25] Source : https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/provv-110413/index.html

1. Contexte réglementaire

A la suite d'une audition publique menée en décembre 2015 et janvier 2016, l'Autorité Fédérale de Surveillance des Marchés Financiers (FINMA) a publié le 3 mars 2016 une circulaire relative aux « *obligations de diligence lors de l'établissement de relations d'affaires par le biais de canaux numérique*s »[26].

La vérification d'identité par vidéo est assimilée à une vérification d'identité en présence de la personne sous réserve qu'elle réponde aux critères techniques et organisationnels suivants :

a. L'identité est vérifiée par le biais d'une communication audiovisuelle en temps réel, au moyen de supports techniques appropriés garantissant une transmission sûre des données et la lecture et le déchiffrage de la zone lisible par machine (MRZ) du document d'identification.
b. L'identification est effectuée par un collaborateur ayant suivi une formation appropriée.
c. Un enregistrement audio de l'entretien est réalisé.
d. L'identification est effectuée selon une procédure précise, comprenant notamment :
    - la transmission par le client de données d'identification en amont de l'entretien audiovisuel ;
    - l'accord exprès du client pour la vérification d'identité par vidéo et l'enregistrement audio de l'entretien ;
    - la prise de photographies du client ainsi que des pages importantes de sa pièce d'identité,
    - le contrôle de l'authenticité de la pièce d'identité par lecture et déchiffrage de la bande MRZ et à l'aide de l'une des marques optiques du document ;
    - la constitution d'un dossier pour chaque vérification d'identité, auquel sont joints les photographies de la pièce d'identité et celles prises au cours de l'entretien audiovisuel ainsi que l'enregistrement audio.

[26] *Circulaire FINMA 2016/7 – Identification par vidéo et en ligne* – Source : https://www.finma.ch/fr/news/2016/03/20160317-mm-fintech/