Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circulaire 2016/7 «Identification par vidéo et en ligne» – révision partielle

Rapport sur les résultats de l'audition qui a eu lieu du 16 décembre 2025 au 27 février 2026

23 septembre 2026

Laupenstrasse 27, 3003 Berne, Tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

Éléments essentiels **4**

Abréviations **5**

1 Introduction **6**

2 Prises de position reçues **6**

3 Résultats de l'audition et évaluation par la FINMA **7**

3.1 Vérification d'identité par vidéo (Cm 5 à 28) 7

3.1.1 Vérification d'identité: autorisation de l'e-ID en tant que document d'identification (Cm 5 à 17) 7

3.1.2 Autorisation des documents d'identification avec code QR (Cm 6, 14, 15) 8

3.2 Vérification d'identité en ligne (Cm 29 à 44.4) 9

3.2.1 Autorisation des documents d'identification avec code QR (Cm 31.3, 32) 9

3.2.2 Virement bancaire (Cm 33) 9

3.2.3 Vérification de l'adresse de domicile (Cm 34 à 37.1) 11

3.2.4 Identification en ligne dans le cas de personnes morales et de sociétés de personnes (Cm 43.1) 12

3.2.5 Identification en ligne au moyen d'une copie électronique d'un document d'identification avec signature électronique qualifiée (Cm 38, 39) 12

3.2.6 Vérification d'identité en ligne au moyen d'une copie électronique du document d'identification avec signature électronique qualifiée et e-ID – vérification supplémentaire du domicile (Cm 38, 39, 44.3) 13

3.2.7 Vérification d'identité en ligne au moyen d'une copie électronique du document d'identification avec signature électronique qualifiée et e-ID – *liveness detection* supplémentaire (Cm 38, 39, 44.3) 14

3.3 Autres préoccupations 15

3.3.1 Effets de la circulaire 15

3.3.2 Équivalence des moyens d'identification électroniques au sens du règlement e-IDAS 15
3.3.3 Liste d'éléments d'identification et de vérification possibles 16

4 Suite de la procédure 17

Éléments essentiels

1. La FINMA a mené, du 15 décembre 2025 au 27 février 2026, une audition publique relative à son projet de révision partielle de la circulaire 2016/7 «Identification par vidéo et en ligne».

2. Le public a largement fait usage de la possibilité de prendre position. Ont notamment participé à cette audition des associations professionnelles et des groupes d'intérêt du secteur financier et des Fintech, des banques et des prestataires de services d'identification.

3. Le projet a en principe été salué. Le souhait d'une reconnaissance plus large de l'e-ID a notamment été exprimé. Celle-ci devrait également pouvoir être utilisée dans le cadre de la vérification d'identité par vidéo.

4. Les participants à l'audition ont majoritairement rejeté l'exigence d'une vérification supplémentaire du domicile lors de l'utilisation d'une signature électronique qualifiée (SEQ) ou d'une e-ID dans le cadre de la vérification d'identité en ligne. Par ailleurs, la vulnérabilité à la fraude de la vérification du domicile, et en particulier des *utility bills*, a été soulignée à plusieurs reprises. Afin de permettre une vérification numérique de bout en bout, il a été proposé d'autoriser des procédures numériques équivalentes. Cette possibilité est désormais prise en compte dans la circulaire.

5. Certains participants à l'audition se sont aussi prononcés en faveur de la mise en place généralisée d'une *liveness detection* en tant qu'élément de sécurité supplémentaire, afin de faire face aux risques croissants de fraude liés aux nouvelles technologies. Cette proposition sera mise en œuvre. La *liveness detection* constitue un outil indispensable pour détecter les hypertrucages (*deepfakes*) et les contrefaçons générées par l'IA.

6. La Circ.-FINMA 16/7 partiellement révisée entrera en vigueur le 1er novembre 2026.

Abréviations

Code QR	Code *quick response*. Code matriciel qui peut être lu avec un *smartphone* ou un autre appareil.
e-ID	Preuve d'identité électronique selon la LeID
LB	Loi du 8 novembre 1934 sur les banques (RS *952.0*)
LBA	Loi du 10 octobre 1997 sur le blanchiment d'argent (RS *955.0*)
LeID	Loi fédérale du 20 décembre 2024 sur l'identité électronique et d'autres moyens de preuves électroniques (loi sur l'e-ID; FF *2025 20*)
MRZ	*Machine readable zone*. Partie visible d'un document d'identité spécialement conçue pour être lue par reconnaissance optique de caractères.
Puce NFC	Une puce *near field communication* permet l'échange de données sans fil sur de très courtes distances, généralement de quelques centimètres seulement.
Règlement e-IDAS	Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73
SEQ	Signature électronique qualifiée
SCSE	Loi du 18 mars 2016 sur la signature électronique (RS *943.03*)
vLEI	Un *verifiable Legal Entity Identifier* est une identité numérique décentralisée qui permet de vérifier l'identité, l'autorité et le rôle des personnes agissant au nom d'une personne morale.

1 Introduction

Du 15 décembre 2025 au 27 février 2026, la FINMA a mené une audition publique sur son projet de révision partielle de la circulaire 2016/7 «Identification par vidéo et en ligne».

Cette révision partielle a pour objectif de tenir compte, dans la circulaire, de l'e-ID selon la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (LeID) qui sera introduite à moyen terme, ainsi que d'autres évolutions technologiques et adaptations administratives.

Le présent rapport expose, sous une forme générale et résumée, les avis émis par les participants à l'audition relative au projet soumis à audition et commente certaines dispositions lorsque cela est nécessaire.

2 Prises de position reçues

Les sociétés, associations, établissements et personnes suivants ont remis une prise de position dans le cadre de l'audition et ont accepté que celle-ci soit publiée[1] (mentionnés par ordre alphabétique):

- AsyLex
- Crypto Valley Association (CVA)
- Digital Identity and Data Sovereignty Association (DIDAS)
- Eurospider Information Technology AG
- EXPERTsuisse
- fidentity AG
- Forum Suisse des organismes d'autorégulation (Forum-OAR)
- Euodia Guthrie
- Intrum SA
- mesoneer AG
- OpenBankingProject.ch
- PXL Vision AG
- Société coopérative Raiffeisen Suisse
- Association suisse des banquiers (ASB)
- Organisme d'autorégulation de l'Association Suisse des Sociétés de Leasing (OAR / ASSL)

[1] Ne sont pas mentionnés ici les participants à l'audition qui n'ont pas souhaité la publication de leur prise de position par la FINMA.

- Organisme d'autorégulation de l'Association Suisse d'Assurances (OAR-ASA)
- Swiss Blockchain Federation (SBF)
- Swiss Fintech Alliance (SFA)
- Swiss Fintech Innovations (SFTI)
- Swiss Payment Association (SPA)
- Swissquote Bank SA
- The Good Token Society Association
- True Wealth SA
- Association Suisse des Gérants de Fortune (ASG)

3 Résultats de l'audition et évaluation par la FINMA

Les prises de position reçues sont résumées, pondérées et évaluées par la FINMA dans le présent rapport. Sauf mention contraire, les références se rapportent aux chiffres marginaux de la version de la circulaire qui a été soumise à audition.

Ce rapport a été approuvé par le conseil d'administration de la FINMA (art. 11 al. 4 de l'ordonnance du 13 décembre 2019 relative à la loi sur la surveillance des marchés financiers; RS *956.11*). Il est publié en même temps que la réglementation adoptée, les explications et les prises de position reçues lors de l'audition.

Les résultats de l'audition et leur appréciation par la FINMA sont présentés ci-après de façon thématique. L'ordre de présentation des thèmes suit celui des chiffres marginaux de la circulaire. Les sujets qui ne se rapportent pas directement à des chiffres marginaux spécifiques ou à la circulaire figurent à la fin du chapitre.

3.1 Vérification d'identité par vidéo (Cm 5 à 28)

3.1.1 Vérification d'identité: autorisation de l'e-ID en tant que document d'identification (Cm 5 à 17)

Prises de position

Les participants à l'audition ont dans l'ensemble salué l'orientation générale de la révision partielle et soutiennent une évolution neutre sur le plan technologique, fondée sur les risques et adaptée à la pratique de la circulaire FINMA 2016/7 «Identification par vidéo et en ligne». Par ailleurs, plusieurs participants à l'audition ont estimé que les nouveaux moyens

d'identification et les nouvelles procédures devraient être autorisés de manière générale, pour autant qu'ils garantissent un niveau de sécurité équivalent.

Étant donné que l'e-ID selon la LeID sera désormais reconnue comme alternative à part entière aux documents d'identité physiques, plusieurs participants à l'audition ont demandé que la circulaire reflète cette équivalence pour tous les canaux de vérification d'identité. Concrètement, l'e-ID devrait être explicitement reconnue non seulement pour la vérification d'identité en ligne, mais aussi pour la vérification d'identité par vidéo. Étant donné que, sur le plan juridique, la vérification d'identité par vidéo est assimilée à une comparution en personne, il n'y aurait aucune raison objective d'exclure un document numérique vérifié par l'État (e-ID) dans les cas où un document physique est admis.

Appréciation

Le traitement différencié de l'e-ID tient compte des différents risques liés aux différents processus de vérification d'identité. Selon la pratique de surveillance en vigueur de la FINMA, la vérification d'identité par vidéo est assimilée à une comparution en personne. Cette équivalence repose sur l'hypothèse qu'il est possible de vérifier visuellement un document d'identité et d'évaluer de manière suffisante ses caractéristiques de sécurité. En matière de vérification d'identité, il n'est pas possible de traiter l'e-ID de la même manière que les documents d'identité classiques. En effet, l'e-ID ne comporte ni MRZ pouvant être lue ou déchiffrée, ni code QR, et il n'est pas non plus possible d'en faire une copie et de l'archiver. Par ailleurs, dans le contexte de l'e-ID, il n'est pas pertinent d'exiger de l'intermédiaire financier qu'il prenne, pendant la transmission vidéo, des photographies «de toutes les pages importantes» de l'e-ID. Dans ce contexte, il semble opportun de ne pas étendre l'utilisation de l'e-ID à la vérification d'identité par vidéo.

Conclusion

L'e-ID est autorisée exclusivement pour la vérification d'identité en ligne.

3.1.2 Autorisation des documents d'identification avec code QR (Cm 6, 14, 15)

Prises de position

De nombreux participants à l'audition ont expressément salué le fait que l'actuelle révision partielle autorise à des fins de vérification d'identité l'utilisation de documents d'identifications comportant un code QR.

Dans un souci de neutralité technologique, il a été suggéré à plusieurs reprises de ne pas limiter la disposition en question exclusivement aux MRZ

et aux codes QR, mais de la formuler de manière plus ouverte ou plus neutre. Cela permettrait de prendre en compte de futures technologies de transmission et de vérification sécurisées des données d'identité (p. ex. les codes Data Matrix ou des solutions ayant des fonctions comparables).

Appréciation

La FINMA adopte en principe une approche neutre sur le plan technologique et estime donc que la nécessité de formuler cette disposition de manière technologiquement neutre est compréhensible. Du point de vue de la FINMA, des prescriptions claires sont toutefois nécessaires pour garantir une mise en œuvre cohérente des documents d'identification autorisés. Les procédures de vérification d'identité doivent par ailleurs être contrôlées au sens de la LBA et leur sécurité doit pouvoir être validée.

Une disposition générale laissant la porte ouverte aux technologies futures renforcerait toutefois les incertitudes concernant les procédures, l'interprétation et l'application du droit, raison pour laquelle il y est renoncé.

La FINMA suit toutefois de près les évolutions techniques et évalue régulièrement si de nouvelles technologies ou des optimisations de processus peuvent être autorisées dans le cadre de la circulaire. La neutralité technologique et l'ouverture à l'innovation continueront donc d'être prises en compte à l'avenir dans le cadre de révisions partielles.

Conclusion

Il est renoncé à autoriser d'autres technologies (futures) que la MRZ et le code QR.

3.2 Vérification d'identité en ligne (Cm 29 à 44.4)

3.2.1 Autorisation des documents d'identification avec code QR (Cm 31.3, 32)

Voir les explications au chapitre 3.1.2.

3.2.2 Virement bancaire (Cm 33)

Prises de position

Concernant le virement bancaire, certains participants à l'audition ont suggéré de ne pas limiter le champ d'application aux banques et aux personnes visées à l'art. 1*b* LB, mais de reconnaître aussi comme preuve valable les virements effectués depuis ou vers des maisons de titres ou des prestataires de services de paiement tels que les émetteurs de cartes de

crédit, Twint, PayPal ou des VASP. Un participant à l'audition a par ailleurs demandé à ce qu'il soit de manière générale renoncé aux virements bancaires.

Une partie des participants à l'audition a en principe salué la possibilité d'effectuer des virements bancaires dans le sens inverse. Toutefois, l'ASB a souligné les risques d'abus liés à la transmission d'un code d'identification, d'autant plus que, dans de telles situations, une banque destinataire ne procède pas nécessairement à une vérification des données des titulaires de comptes et qu'elle devrait, dans le cadre du monitorage des transactions, contrôler ces virements afin de détecter d'éventuelles opérations frauduleuses. Dans le cadre du virement bancaire dans le sens inverse, il existerait un risque qu'un client potentiel indique un compte quelconque auprès d'une banque tierce et transmette ensuite à un tiers le code d'identification ainsi communiqué. Pour faire face à ces risques de manière adéquate, une banque destinataire devrait prévoir des mesures supplémentaires, ce qui entraînerait pour elle une charge opérationnelle et administrative supplémentaire (notamment la nécessité de vérifier les données des titulaires de comptes ainsi qu'une charge supplémentaire liée au monitorage des transactions).

Appréciation

Le champ d'application de l'élément de sécurité du virement a été délibérément limité aux banques, y compris les personnes visées à l'art. 1*b* LB. Concernant les banques en Suisse, au Liechtenstein ou dans un État membre du GAFI qui satisfait aux exigences énoncées au Cm 33, il est garanti que l'identité a déjà été vérifiée de manière suffisante. Eu égard au cadre complet du droit de la surveillance et en matière de lutte contre le blanchiment d'argent, une autorisation bancaire offre une base de confiance réglementaire accrue; le virement bancaire peut ainsi être pris en compte dans la circulaire comme élément de sécurité supplémentaire.

Renoncer complètement au virement bancaire, sans mettre en place d'autres mesures de sécurité complémentaires telles que la lecture de la puce des documents d'identification biométriques, réduirait considérablement la sécurité de la vérification d'identité en ligne et augmenterait le risque de fraude.

L'introduction du virement bancaire dans le sens inverse initialement proposée par la branche devait offrir aux établissements une alternative au virement bancaire conventionnel . Les doutes formulés par l'ASB indiquent qu'il n'existe toujours pas d'accord sur cet élément de sécurité alternatif. En raison des réserves exprimées, le virement bancaire dans le sens inverse ne sera pas introduit.

Conclusion

Le virement bancaire dans le sens inverse n'est pas introduit. Le champ d'application du Cm 33 reste limité aux banques, y compris les personnes visées à l'art. 1*b* LB.

3.2.3 Vérification de l'adresse de domicile (Cm 34 à 37.1)

Prises de position

Plusieurs participants à l'audition ont souligné que les méthodes prévues dans la circulaire concernant l'attestation de domicile étaient techniquement obsolètes et peu fiables. Certains ont proposé d'autoriser également des justificatifs numériques équivalents pour l'attestation de domicile. Un participant à l'audition a aussi mentionné dans ce contexte les attestations établies par voie numérique par les communes de domicile ou les autorités compétentes.

Appréciation

La FINMA partage l'avis selon lequel les *utility bills*, par exemple, sont susceptibles d'être falsifiées et comprend la nécessité de pouvoir s'appuyer sur des processus numériques de bout en bout pour l'attestation de domicile aussi. Il existe maintenant des processus numériques qui permettent d'identifier de manière fiable les cocontractants, leur domicile et leurs infrastructures. La circulaire autorise donc désormais explicitement le recours à des procédures numériques équivalentes pour la vérification du domicile. La géolocalisation faisant partie de ces méthodes numériques équivalentes, elle n'est plus mentionnée explicitement dans la circulaire.

Selon la circulaire, il était déjà possible jusqu'à présent d'utiliser des extraits de registres publics délivrés par voie numérique par les autorités comme attestations de domicile pour la vérification du domicile.

Conclusion

Les procédures numériques équivalentes, qui permettent d'attribuer de manière fiable un lieu de domicile au cocontractant et à son infrastructure, sont autorisées pour la vérification du domicile.

3.2.4 Identification en ligne dans le cas de personnes morales et de sociétés de personnes (Cm 43.1)

Prises de position

Les participants à l'audition ont majoritairement salué le fait que l'e-ID soit aussi autorisée pour l'ouverture de relations d'affaires par voie numérique avec des personnes morales ou des sociétés de personnes. Dans ce contexte, le *verifiable LEI* (vLEI) a été cité comme un outil adapté à la représentation numérique de personnes morales et de leurs rapports de représentation. Il a aussi été suggéré de préciser qu'aucune vérification supplémentaire du domicile n'était nécessaire pour les personnes agissant au nom de personnes morales ou de sociétés de personnes.

Appréciation

Dans le cas des personnes morales ou des sociétés de personnes, il y a lieu de vérifier l'identité des personnes physiques qui établissent la relation d'affaires. Le *verifiable LEI* peut certes contribuer à la représentation numérique des personnes morales ainsi que de leurs rapports de représentation, mais il ne remplace pas la vérification d'identité des personnes physiques.

La vérification de l'adresse de domicile constitue, dans le cadre de la vérification d'identité de personnes physiques, un élément de sécurité supplémentaire visant à réduire les risques d'usurpation d'identité; elle est en principe prévue dans le cadre de l'identification en ligne. L'ouverture de relations d'affaires avec des personnes morales peut avoir lieu à tout moment conformément aux dispositions déjà en vigueur des Cm 40 et 41 (sans vérification du domicile).

Conclusion

Le Cm 43.1 n'est pas adapté.

3.2.5 Identification en ligne au moyen d'une copie électronique d'un document d'identification avec signature électronique qualifiée (Cm 38, 39)

Prises de position

Un participant à l'audition a suggéré d'accepter de manière générale les signatures électroniques liées à l'identité, assorties d'une piste d'audit *(audit trail)* claire, d'une garantie d'intégrité et d'horodatage, ainsi que d'une traçabilité évidente de la déclaration en tant qu'alternative équivalente à la SEQ.

Appréciation

Une SEQ au sens de la loi sur la signature électronique (SCSE, RS *943.03*) garantit un niveau élevé de vérification d'identité. Les signatures sophistiquées ne comportent souvent pas les mêmes éléments de sécurité institutionnels et réglementaires que la SEQ. Une SEQ fondée sur la SCSE offre un standard uniforme ancré dans la loi et une grande sécurité juridique. Il est donc renoncé à une extension à d'autres types de signatures.

Conclusion

La vérification d'identité en ligne avec une SEQ ne sera pas étendue à d'autres signatures.

3.2.6 Vérification d'identité en ligne au moyen d'une copie électronique du document d'identification avec signature électronique qualifiée et e-ID – vérification supplémentaire du domicile (Cm 38, 39, 44.3)

Prises de position

Les participants à l'audition ont majoritairement critiqué le fait qu'une vérification supplémentaire du domicile soit prévue dans le cadre de la vérification d'identité en ligne avec une SEQ ou au moyen de l'e-ID.

Un participant a notamment fait valoir que les procédures techniques employées (*liveness check*, *face matching*, validation conforme aux standards ETSI) utilisées lors de la vérification d'identité en vue de l'obtention d'une SEQ offraient déjà un niveau de sécurité plus élevé quant à l'existence réelle de la personne à identifier que ce que prévoit la circulaire pour la vérification d'identité au moyen d'une copie ordinaire d'un document d'identification avec vérification de l'authenticité par l'intermédiaire financier. Une vérification supplémentaire du domicile ne serait pas nécessaire et n'apporterait aucune valeur ajoutée du point de vue de la prévention du blanchiment d'argent. Par ailleurs, un délai transitoire approprié a été demandée pour permettre les éventuelles adaptations techniques nécessaires.

Appréciation

Comme indiqué dans les explications, la vérification d'identité en ligne avec la SEQ ou au moyen de l'e-ID doit être qualifiée d'ouverture par voie de correspondance. Conformément à l'art. 45 al. 2 OBA-FINMA, l'adresse de domicile doit donc être vérifiée par un moyen approprié. La vérification du domicile constitue de manière générale un élément de sécurité supplémentaire dans le cadre de la vérification d'identité en ligne. Elle constitue un obstacle supplémentaire pour les fraudeurs potentiels,

puisqu'ils doivent fournir une preuve plausible du domicile en plus de l'identité. Cela complique les ouvertures de compte frauduleuses, demande davantage de travail pour réaliser des opérations frauduleuses et peut ainsi avoir un effet dissuasif.

Les préoccupations des participants à l'audition sont prises en compte en ce sens qu'un délai transitoire de douze mois est prévu pour les adaptations techniques liées à la vérification du domicile dans le cadre de la vérification d'identité avec une SEQ.

Conclusion

L'obligation de vérification du domicile est maintenue. Un délai transitoire de douze mois est accordé pour les adaptations techniques liées à la vérification du domicile dans le cadre de la vérification d'identité avec une SEQ.

3.2.7 Vérification d'identité en ligne au moyen d'une copie électronique du document d'identification avec signature électronique qualifiée et e-ID – *liveness detection* supplémentaire (Cm 38, 39, 44.3)

Prises de position

En lien avec la vérification du domicile, plusieurs participants à l'audition ont souligné le risque accru de falsification, notamment dû à l'utilisation d'outils d'IA, ainsi que l'usurpation d'identité par le biais d'opérations frauduleuses fondées sur l'hypertrucage. Afin de réduire ce risque, ils ont proposé de mettre en place une *liveness detection* en complément de la vérification du domicile.

Appréciation

Comme le souligne la FINMA dans sa communication sur la surveillance 02/2026, les risques de fraude numérique sont bien réels notamment dans le cadre de l'ouverture numérique de relations clients. Compte tenu de l'augmentation avérée des risques liés aux nouvelles technologies, il semble donc opportun d'adapter la *liveness detection*, déjà prévue au Cm 32, aux autres variantes de vérification d'identité en ligne.

La *liveness detection* compte sur le marché comme élément de sécurité efficace pour renforcer la sécurité des processus de vérification d'identité et lutter contre les hypertrucages et les falsifications fondées sur l'IA. Cette appréciation a été confirmée par plusieurs contributions dans le cadre de l'audition publique. Combinée à la vérification du domicile, la *liveness detection* renforce ainsi le niveau de sécurité lors de la vérification d'identité en ligne et permet de faire face aux risques croissants de fraude.

Conclusion

L'exigence d'une *liveness detection* est ajoutée aux Cm 39 et 44.3 en lien avec la vérification d'identité en ligne au moyen d'une copie électronique du document d'identification avec SEQ et e-ID.

3.3 Autres préoccupations

3.3.1 Effets de la circulaire

Prises de position

Un participant à l'audition a fait valoir que les tentatives de fraude dans le domaine numérique, notamment celles impliquant l'IA et l'utilisation abusive des données, devenaient de plus en plus complexes. Pour faire face aux risques qui en découlent, les dispositions actuelles de la circulaire s'avéreraient souvent insuffisantes et devraient être complétées par des mesures supplémentaires selon une approche fondée sur les risques. La FINMA devrait donc préciser que la circulaire définit des exigences minimales qui seraient à compléter en fonction des risques.

Appréciation

La FINMA partage l'avis selon lequel les dispositions d'exécution de la circulaire doivent être considérées comme des exigences minimales. En fonction de la situation en matière de risques et du modèle d'affaires de l'intermédiaire financier, des mécanismes de sécurité supplémentaires peuvent être nécessaires. Il n'est toutefois pas nécessaire d'apporter de précisions explicites dans la circulaire, d'autant plus que la pratique qui y est définie doit toujours être considérée comme un minimum et que des mesures de sécurité supplémentaires découlent notamment de la nécessité d'une gestion adéquate des risques.

Conclusion

Aucune modification n'est apportée à la circulaire.

3.3.2 Équivalence des moyens d'identification électroniques au sens du règlement e-IDAS

Prises de position

Plusieurs participants à l'audition ont demandé que les moyens d'identification électroniques délivrés par les États membres de l'UE conformément au règlement e-IDAS soient reconnus comme équivalents. Le

but serait d'éviter les obstacles réglementaires et les ruptures de continuité dans le processus d'*onboarding* transfrontière des clients.

Appréciation

La prise en compte des moyens d'identification électroniques selon le règlement e-IDAS nécessite un cadre technique et réglementaire au niveau international. Si le règlement e-IDAS établit un cadre uniforme pour la reconnaissance, à l'échelle de l'UE, des identités numériques à différents niveaux de confiance, la solution suisse est, pour l'instant, conçue comme un système national, proche de l'État, et ancrée dans la loi. Une e-ID suisse n'est pas automatiquement reconnue comme équivalente dans les relations juridiques avec l'UE. De même, les moyens d'identification électroniques au sens du règlement e-IDAS ne peuvent être admis en Suisse pour la vérification numérique de l'identité des cocontractants au sens de la circulaire sans un examen technique et réglementaire approfondi.

Conclusion

Une reconnaissance d'équivalence des moyens d'identification électroniques délivrés selon le règlement e-IDAS n'est actuellement pas prévue.

3.3.3 Liste d'éléments d'identification et de vérification possibles

Prises de position

Un participant à l'audition a suggéré de ne pas réglementer dans la circulaire les détails relatifs à l'identification par vidéo et en ligne, mais de fournir aux intermédiaires financiers une liste non exhaustive d'éléments d'identification et de vérification possibles. Il appartiendrait alors en fin de compte aux intermédiaires financiers, selon leur appréciation et sous leur responsabilité, de déterminer comment respecter les obligations de diligence prévues par la LBA selon une approche fondée sur les risques.

Appréciation

La FINMA adopte certes une approche réglementaire fondée sur des principes et neutre sur le plan technologique, qui permet aux intermédiaires financiers d'utiliser différentes solutions technologiques pour la vérification numérique de l'identité des cocontractants. Les exigences de la LBA et de l'OBA-FINMA doivent cependant être transposées au contexte numérique. Des normes minimales prudentielles sont donc nécessaires pour garantir une pratique de surveillance cohérente ainsi qu'un niveau de sécurité et de confiance uniforme et suffisant pour respecter les exigences de la LBA.

Conclusion

Une liste non exhaustive d'éléments d'identification et de vérification possibles n'est pas établie.

4 Suite de la procédure

La Circ.-FINMA 16/7 partiellement révisée entrera en vigueur le 1er novembre 2026.

Des délais transitoires d'un an à compter de l'entrée en vigueur s'appliquent concernant la garantie de la vérification du domicile dans le cadre de la vérification d'identité en ligne avec une SEQ.