

Rundschreiben 2016/7 «Video- und Online-Identifi- zierung» – Teilrevision

Bericht über die Ergebnisse der Anhörung vom 16. Dezember
2025 bis 27. Februar 2026

23. September 2026

Inhaltsverzeichnis

Kernpunkte.....	4
Abkürzungsverzeichnis	5
1 Einleitung.....	6
2 Eingegangene Stellungnahmen	6
3 Ergebnisse der Anhörung und Beurteilung durch die FINMA	7
3.1 Video-Identifizierung (Rz 5–28).....	7
3.1.1 Identitätsprüfung: Zulassung der E-ID als Identifizierungsdokument (Rz 5–17).....	7
3.1.2 Zulassung von Identifizierungsdokumenten mit QR- Code (Rz 6, 14, 15)	8
3.2 Online-Identifizierung (Rz 29–44.4)	9
3.2.1 Zulassung von Identifizierungsdokumenten mit QR- Code (Rz 31.3, 32)	9
3.2.2 Banküberweisung (Rz 33)	9
3.2.3 Prüfung der Wohnsitzadresse (Rz 34–37.1)	11
3.2.4 Online-Identifizierung bei juristischen Personen und Personengesellschaften (Rz 43.1)	11
3.2.5 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur (Rz 38, 39)	12
3.2.6 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur und E-ID – zusätzliche Wohnsitzprüfung (Rz 38, 39, 44.3).....	13
3.2.7 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur und E-ID – zusätzliche <i>Liveness Detection</i> (Rz 38, 39, 44.3).....	14
3.3 Weitere Anliegen	15
3.3.1 Wirkung des Rundschreibens	15

3.3.2	Gleichstellung von elektronischen Identifizierungsnachweisen gemäss eIDAS- Verordnung	15
3.3.3	Katalog von möglichen Identifizierungs- und Verifikationselementen	16
4	Weiteres Vorgehen	17

Kernpunkte

1. Vom 16. Dezember 2025 bis 27. Februar 2026 führte die FINMA eine öffentliche Anhörung zum Entwurf des teilrevidierten Rundschreibens 2016/7 «Video- und Online-Identifizierung» durch.
2. Die Möglichkeit zur Stellungnahme wurde von der Öffentlichkeit rege genutzt. An der Anhörung haben unter anderem Branchen- und Interessenverbände des Finanz- und Fintech-Sektors, Banken und Identifizierungsdienstleister teilgenommen.
3. Die Vorlage wurde grundsätzlich unterstützt. Geäussert wurde insbesondere der Wunsch nach einer umfassenderen Anerkennung der E-ID. Diese solle auch im Rahmen der Video-Identifizierung eingesetzt werden können.
4. Die Anforderung der zusätzlichen Wohnsitzprüfung beim Einsatz einer QES oder E-ID im Rahmen einer Online-Identifizierung wurde in der Anhörung mehrheitlich abgelehnt. Zudem wurde mehrfach auf die Betrugsanfälligkeit der Wohnsitzprüfung und insbesondere der *Utility Bills* hingewiesen und vorgeschlagen, zur Vermeidung von Medienbrüchen auch gleichwertige digitale Verfahren zuzulassen, was neu im Rundschreiben berücksichtigt wird.
5. Auch haben sich einige Anhörungsteilnehmende dafür ausgesprochen, generell eine *Liveness Detection* als zusätzliches Sicherheitselement vorzusehen, um die steigenden Betrugsrisiken durch die neuen Technologien zu adressieren. Dieser Vorschlag wird umgesetzt. Die *Liveness Detection* stellt ein notwendiges Mittel dar, um *Deepfakes* und KI-gestützte Fälschungen erkennen zu können.
6. Das teilrevidierte FINMA-RS 16/7 tritt am 1. November 2026 in Kraft.

Abkürzungsverzeichnis

BankG	Bankengesetz vom 8. November 1934 (SR 952.0)
BGEID	Bundesgesetz vom 20. Dezember 2024 über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz; BBl 2025 20)
E-ID	Elektronischer Identitätsnachweis nach BGEID
eIDAS-Verordnung	<i>electronic Identification, Authentication and trust Services</i> , Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73
GwG	Geldwäschereigesetz vom 10. Oktober 1997 (SR 955.0)
MRZ	<i>Machine Readable Zone</i> . Sichtbarer Teil eines Ausweisdokumentes, der speziell dafür ausgelegt wurde, durch optische Texterkennung gelesen zu werden
NFC-Chip	Ein <i>Near Field Communication</i> -Chip ermöglicht den drahtlosen Datenaustausch über sehr kurze Distanzen von meist nur wenigen Zentimetern
QES	Qualifizierte elektronische Signatur
QR-Code	<i>Quick Response Code</i> . Matrixcode, der durch Scannen mit einem Smartphone oder anderem Gerät ausgelesen werden kann
vLEI	Ein <i>verifiable Legal Entity Identifier</i> ist eine dezentralisierte digitale Identität, die es ermöglicht, die Identität, Autorität und Rolle von Personen, die im Namen einer juristischen Person handeln, zu überprüfen.
ZertES	Bundesgesetz vom 18. März 2016 über die elektronische Signatur (SR 943.03)

1 Einleitung

Vom 16. Dezember 2025 bis 27. Februar 2026 führte die FINMA eine öffentliche Anhörung zum Entwurf des teilrevidierten Rundschreibens 2016/7 «Video- und Online-Identifizierung» durch.

Zielsetzung der Teilrevision ist es, die E-ID nach dem Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID), welche mittelfristig eingeführt wird, sowie weitere technologische Entwicklungen und administrative Anpassungen im Rundschreiben zu berücksichtigen.

Der vorliegende Bericht geht in allgemeiner und zusammengefasster Form auf die eingegangenen Stellungnahmen der Anhörungsteilnehmenden zum Anhörungsentwurf ein und erläutert, wo angebracht, einzelne Bestimmungen.

2 Eingegangene Stellungnahmen

Folgende Gesellschaften, Verbände, Institute und Personen haben im Rahmen der Anhörung eine Stellungnahme eingereicht und sich für deren Publikation¹ ausgesprochen (in alphabetischer Reihenfolge):

- AsyLex
- Crypto Valley Association (CVA)
- Digital Identity and Data Sovereignty Association (DIDAS)
- Eurospider Information Technology AG
- EXPERTsuisse
- Fidentity AG
- Forum Schweizer Selbstregulierungsorganisationen (Forum-SRO)
- Euodia Guthrie
- Intrum AG
- Mesoneer AG
- OpenBankingProject.ch
- PXL Vision AG
- Raiffeisen Schweiz Genossenschaft
- Schweizerische Bankiervereinigung (SBVg)

¹ Nicht aufgeführt sind diejenigen Anhörungsteilnehmenden, die sich gegen eine Veröffentlichung ihrer Stellungnahme durch die FINMA ausgesprochen haben.

- Selbstregulierungsorganisation des Schweizerischen Leasingverbandes (SRO/SLV)
- Selbstregulierungsorganisation des Schweizerischen Versicherungsverbandes (SRO-SVV)
- Swiss Blockchain Federation (SBF)
- Schweizer Fintech Alliance (SFA)
- Swiss Fintech Innovations (SFTI)
- Swiss Payment Association (SPA)
- Swissquote Bank SA
- The Good Token Society Association
- True Wealth AG
- Verband Schweizerischer Vermögensverwalter (VSV)

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA

Im vorliegenden Bericht werden die eingegangenen Stellungnahmen von der FINMA zusammengefasst, gewichtet und ausgewertet. Ohne weitere Angabe beziehen sich die Verweise auf Randziffern der Anhörungsversion des Rundschreibens.

Der Bericht wurde vom Verwaltungsrat der FINMA verabschiedet (Art. 11 Abs. 4 der Verordnung vom 13. Dezember 2019 zum Finanzmarktaufsichtsgesetz; SR 956.11). Er wird zusammen mit den verabschiedeten Regulierungen, den Erläuterungen und den Stellungnahmen aus der Anhörung veröffentlicht.

Die Ergebnisse der Anhörung und die Beurteilung durch die FINMA werden nachfolgend nach Themenblöcken gegliedert dargestellt. Die Abfolge der Themenblöcke entspricht der Reihenfolge der Randziffern des Rundschreibens. Themen, die sich nicht direkt auf einzelne Randziffern oder das Rundschreiben beziehen, sind am Ende des Kapitels aufgeführt.

3.1 Video-Identifizierung (Rz 5–28)

3.1.1 Identitätsprüfung: Zulassung der E-ID als Identifizierungsdokument (Rz 5–17)

Stellungnahmen

Die Anhörungsteilnehmenden begrüßten insgesamt die Zielrichtung der Teilrevision und unterstützen eine technologie neutrale, risikobasierte und

praxisnahe Weiterentwicklung des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung». Zudem haben sich diverse Anhörungsteilnehmende dahingehend geäußert, dass neue Identifikationsmittel und Verfahren generell zugelassen werden sollten, sofern sie ein gleichwertiges Sicherheitsniveau gewährleisten.

Da der E-ID gemäss BGEID künftig der Status einer vollwertigen Alternative zu physischen Identitätsdokumenten zugestanden wird, forderten mehrere Anhörungsteilnehmende diese Gleichwertigkeit über alle Identifikationskanäle hinweg im Rundschreiben abzubilden. Konkret solle die E-ID explizit nicht nur für die Online-Identifizierung, sondern auch für die Video-Identifizierung anerkannt werden. Da die Video-Identifizierung rechtlich der persönlichen Vorsprache gleichgestellt ist, gäbe es keinen sachlichen Grund, ein staatlich verifiziertes digitales Dokument (E-ID) dort auszuschliessen, wo ein physisches Dokument zulässig sei.

Würdigung

Die differenzierte Behandlung der E-ID trägt den unterschiedlichen Risiken der einzelnen Identifizierungsprozesse Rechnung. Die Video-Identifizierung ist nach geltender Aufsichtspraxis der FINMA der persönlichen Vorsprache gleichgestellt. Diese Gleichstellung basiert auf der Annahme, dass ein Identifizierungsdokument visuell überprüft und dessen sicherheitsrelevanten Merkmale ausreichend beurteilt werden können. Die E-ID kann im Zusammenhang mit der Identifizierung nicht gleich wie klassische Ausweisdokumente behandelt werden. Namentlich weist die E-ID keine auslesbare bzw. entschlüsselbare MRZ sowie keinen QR-Code auf und es kann keine Ausweiskopie der E-ID erstellt und archiviert werden. Weiter ist es im Kontext der E-ID nicht zweckdienlich, vom Finanzintermediär zu verlangen, dass dieser während der Videoübertragung Lichtbilder «von allen relevanten Seiten» der E-ID erstellt. Vor diesem Hintergrund erscheint es sachgerecht, den Einsatz der E-ID nicht auf die Video-Identifizierung auszuweiten.

Fazit

Die E-ID wird ausschliesslich für die Online-Identifizierung zugelassen.

3.1.2 Zulassung von Identifizierungsdokumenten mit QR-Code (Rz 6, 14, 15)

Stellungnahmen

Zahlreiche Anhörungsteilnehmende begrüßten ausdrücklich, dass im Rahmen der vorliegenden Teilrevision die Nutzung von Ausweisdokumenten mit QR-Code zu Identifizierungszwecken zugelassen werden soll.

Im Sinne der Technologieneutralität wurde vereinzelt angeregt, die entsprechende Bestimmung nicht ausschliesslich auf MRZ und QR-Codes zu begrenzen, sondern offener bzw. neutraler zu formulieren. Dadurch könnten auch zukünftige Technologien zur sicheren Übermittlung und Verifikation von Identitätsdaten (z.B. Data-Matrix-Codes oder funktional vergleichbare Lösungen) erfasst werden.

Würdigung

Die FINMA verfolgt grundsätzlich einen technologieneutralen Ansatz und erachtet daher das Bedürfnis nach einer technologieneutralen Formulierung der Bestimmung als nachvollziehbar. Aus Sicht der FINMA sind jedoch klare Vorgaben erforderlich, um eine konsistente Umsetzung der zugelassenen Identifizierungsdokumente sicherzustellen. Zudem müssen Identifizierungsverfahren im Sinne des GwG überprüfbar und hinsichtlich ihrer Sicherheit validierbar sein.

Eine generalklauselartige Öffnung für zukünftige Technologien würde jedoch die Unsicherheiten hinsichtlich Prozesse, Auslegung und Rechtsanwendung erhöhen, weshalb davon abgesehen wird.

Die FINMA beobachtet allerdings fortlaufend die technischen Entwicklungen und evaluiert auf regelmässiger Basis, ob neue Technologien oder Prozessoptimierungen für das Rundschreiben zugelassen werden können. Der Technologieneutralität und Innovationsoffenheit wird somit auch künftig im Rahmen von Teilrevisionen Rechnung getragen.

Fazit

Auf eine Zulassung weiterer beliebiger (zukünftiger) Technologien neben der MRZ und dem QR-Code wird verzichtet.

3.2 Online-Identifizierung (Rz 29–44.4)

3.2.1 Zulassung von Identifizierungsdokumenten mit QR-Code (Rz 31.3, 32)

Siehe die Ausführungen unter Kapitel 3.1.2.

3.2.2 Banküberweisung (Rz 33)

Stellungnahmen

Zur Banküberweisung regten einzelne Anhörungsteilnehmende an, den Anwendungsbereich nicht auf Banken und Personen nach Art. 1b BankG zu beschränken, sondern auch Überweisungen von/an Wertpapierhäuser oder

Zahlungsdienstleister wie beispielsweise Kreditkartenherausgeber, Twint, Paypal oder VASPs als tauglichen Nachweis anzuerkennen. Eine Eingabe forderte zudem generell auf eine Banküberweisung zu verzichten.

Ein Teil der Anhörungsteilnehmenden begrüßte grundsätzlich die Möglichkeit der umgekehrten Banküberweisung. Hingegen wies die SBVg auf damit verbundene Missbrauchsrisiken im Zusammenhang mit der Übermittlung eines Identifizierungscodes hin, zumal eine Empfängerbank in solchen Konstellationen nicht zwingend einen Abgleich der Kontoinhaberdaten vornehme und dieselbe solche Geldüberweisungen im Rahmen ihres Transaktionsmonitorings auf mögliche betrügerische Machenschaften prüfen müsste. Es bestehe im Zusammenhang mit der «umgekehrten» Banküberweisung das Risiko, dass eine potenzielle Kundin oder ein potenzieller Kunde ein beliebiges Konto bei einer Drittbank angeben und den auf diesem Weg übermittelten Identifizierungscode anschliessend an eine Drittperson weiterleiten könnte. Um diesen Risiken angemessen zu begegnen, müsste eine Empfängerbank zusätzliche Massnahmen vorsehen, was mit entsprechendem operativem und administrativem Mehraufwand für dieselbe verbunden wäre (insbesondere Notwendigkeit zum Abgleich der Kontoinhaberdaten sowie Mehraufwand im Zusammenhang mit dem Transaktionsmonitoring).

Würdigung

Der Anwendungsbereich des Sicherheitselements der Überweisung wurde bewusst auf Banken einschliesslich Personen nach Art. 1b BankG festgelegt. Bei Banken in der Schweiz, Liechtenstein oder einem FATF-Staat, welcher die Vorgaben gemäss Rz 33 erfüllt, ist sichergestellt, dass bereits einmal eine Identifizierung mit ausreichendem Standard vorgenommen wurde. Eine Bankbewilligung bietet aufgrund des umfassenden aufsichts- und geldwäschereirechtlichen Rahmens eine erhöhte regulatorische Vertrauensbasis, weshalb die Banküberweisung als zusätzliches Sicherheitselement im Rundschreiben berücksichtigt werden kann.

Ein gänzlicher Verzicht auf die Banküberweisung, ohne weitere flankierende Sicherheitsmassnahmen wie beispielsweise dem Auslesen des Chips der biometrischen Ausweise, würde die Sicherheit der Online-Identifizierung empfindlich reduzieren und das Betrugsrisiko erhöhen.

Der Anstoss für die Einführung einer umgekehrten Banküberweisung kam ursprünglich aus der Branche und hätte für die Institute eine Alternative zur herkömmlichen Banküberweisung schaffen sollen. Die eingebrachten Bedenken seitens SBVg weisen darauf hin, dass zu diesem alternativen Sicherheitselement noch keine Einigung besteht. Aufgrund der geäusserten Vorbehalte wird auf die Einführung einer «umgekehrten» Banküberweisung verzichtet.

Fazit

Die «umgekehrte» Banküberweisung wird nicht eingeführt. Der Anwendungsbereich von Rz 33 bleibt auf Banken einschliesslich Personen nach Art. 1b BankG beschränkt.

3.2.3 Prüfung der Wohnsitzadresse (Rz 34–37.1)

Stellungnahmen

Verschiedene Anhörungsteilnehmende haben darauf hingewiesen, dass die im Rundschreiben vorgesehenen Methoden für die Wohnsitzbestätigung technisch veraltet und wenig verlässlich seien. Vereinzelt wurde vorgeschlagen, für die Wohnsitzbestätigung auch gleichwertige digitale Nachweise zuzulassen. Eine Eingabe hat hier auch auf digital durch Wohngemeinden oder zuständige Behörden ausgestellte Bestätigungen verwiesen.

Würdigung

Die FINMA teilt die Einschätzung, dass beispielsweise *Utility Bills* fälschungsanfällig sind und versteht das Bedürfnis, auch für die Wohnsitzbestätigung auf digitale Prozesse setzen zu können, die keinen Medienbruch hervorrufen. Mittlerweile existieren digitale Prozesse, die eine sichere Zuordnung von Vertragspartei, deren Wohnsitz und Infrastruktur ermöglichen. Im Rundschreiben werden deshalb gleichwertige digitale Verfahren neu explizit zur Wohnsitzprüfung zugelassen. Da eine Geolokalisierung ebenfalls unter solche gleichwertigen digitalen Verfahren subsumierbar ist, wird diese im Rundschreiben nicht mehr explizit erwähnt.

Digital ausgestellte Wohnsitzbestätigungen von Behörden konnten bereits unter bisherigem Rundschreiben als Ausfluss eines öffentlichen Registers für die Wohnsitzprüfung hinzugezogen werden.

Fazit

Gleichwertige digitale Verfahren, welche die Vertragspartei und deren Infrastruktur zuverlässig einem Wohnsitz zuordnen, werden für die Wohnsitzprüfung zugelassen.

3.2.4 Online-Identifizierung bei juristischen Personen und Personengesellschaften (Rz 43.1)

Stellungnahmen

Ein Grossteil der Anhörungsteilnehmenden begrüsst, dass die E-ID auch für die digitale Eröffnung von Geschäftsbeziehungen mit juristischen Personen oder Personengesellschaften zugelassen wird. In diesem Zusammenhang wurde die *verifiable LEI* (vLEI) als geeignetes Instrument zur digitalen

Abbildung juristischer Personen und ihrer Vertretungsverhältnisse genannt. Zudem wurde angeregt, klarzustellen, dass bei Personen, die im Namen von juristischen Personen oder Personengesellschaften handeln, keine zusätzliche Wohnsitzprüfung erforderlich sei.

Würdigung

Bei juristischen Personen oder Personengesellschaften ist die Identität der natürlichen Personen, welche die Geschäftsbeziehung eröffnen, zu überprüfen. Die *verifiable LEI* kann zwar zur digitalen Abbildung juristischer Personen sowie ihrer Vertretungsverhältnisse beitragen, ersetzt jedoch nicht die Identifizierung der natürlichen Personen.

Die Überprüfung der Wohnsitzadresse ist bei der Identifizierung von natürlichen Personen ein zusätzliches Sicherheitselement zur Verminderung der Risiken von Identitätsmissbrauch und ist bei der Online-Identifizierung grundsätzlich vorgesehen. Die Aufnahme der Geschäftsbeziehungen von juristischen Personen kann jederzeit nach den bereits geltenden Vorgaben in Rz 40 und 41 (ohne Wohnsitzprüfung) erfolgen.

Fazit

Rz 43.1 bleibt unverändert.

3.2.5 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur (Rz 38, 39)

Stellungnahmen

Ein Anhörungsteilnehmer regte an, generell identitätsgebundene elektronische Signaturen mit sauberem Audit-Trail, Integritäts- und Zeitstempelsicherung sowie klarer Nachvollziehbarkeit der Erklärungsabgabe als gleichwertige Alternative zur QES zu akzeptieren.

Würdigung

Eine QES gemäss dem Bundesgesetz über die elektronische Signatur (ZertES, SR 943.03) sichert einen hohen Identifizierungsstandard. Fortgeschrittene Signaturen weisen regelmässig nicht dieselben institutionellen und regulatorischen Sicherheitselemente wie die QES auf. Eine auf dem ZertES basierende QES bietet einen einheitlichen im Gesetz verankerten Standard und eine hohe Rechtssicherheit, weshalb von einer Ausdehnung auf weitere Signaturen abgesehen wird.

Fazit

Die Online-Identifizierung mittels QES wird nicht auf weitere Signaturen erweitert.

3.2.6 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur und E-ID – zusätzliche Wohnsitzprüfung (Rz 38, 39, 44.3)

Stellungnahmen

Die Mehrheit der Anhörungsteilnehmenden kritisierte, dass bei der Online-Identifizierung mittels QES oder E-ID zusätzlich eine Wohnsitzprüfung vorgesehen wird.

Ein Anhörungsteilnehmender argumentierte im Konkreten, dass die eingesetzten technischen Verfahren (*Liveness Check*, *Face Matching*, ETSI-konforme Validierung) bei der Identifizierung zur Erlangung einer QES bereits ein höheres Sicherheitsniveau hinsichtlich der tatsächlichen Existenz einer zu identifizierenden Person biete, als dies im Rundschreiben bei der Identifizierung mittels herkömmlicher Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär vorgesehen sei. Eine zusätzliche Wohnsitzprüfung sei nicht erforderlich und biete keinen Mehrwert aus Sicht der Geldwäschereiprävention. Zudem wurde eine angemessene Übergangsfrist für allfällige erforderliche technische Anpassungen verlangt.

Würdigung

Wie in den Erläuterungen ausgeführt wird, ist die Identifizierung mittels QES oder E-ID als Eröffnung auf dem Korrespondenzweg zu qualifizieren und es ist gemäss Art. 45 Abs. 2 GwV-FINMA die Wohnsitzadresse durch einen entsprechenden Nachweis zu verifizieren. Die Wohnsitzprüfung ist bei der Online-Identifizierung generell ein zusätzliches Sicherheitselement. Sie stellt für potentielle Betrüger eine zusätzliche Hürde dar, da neben der Identität auch ein plausibler Nachweis des Wohnsitzes erbracht werden muss. Dies erschwert missbräuchliche Kontoeröffnungen, erhöht den Aufwand für Täuschungshandlungen und kann dadurch eine abschreckende Wirkung entfalten.

Dem Anliegen der Anhörungsteilnehmenden wird insofern Rechnung getragen, als eine zwölfmonatige Übergangsfrist für die technischen Anpassungen im Zusammenhang mit der Wohnsitzprüfung bei der Identifizierung via QES vorgesehen wird.

Fazit

Am Erfordernis der Wohnsitzprüfung wird festgehalten. Es wird eine Übergangsfrist von zwölf Monaten für die technischen Anpassungen bei der Identifizierung via QES gewährt.

3.2.7 Online-Identifizierung mittels elektronischer Ausweiskopie mit qualifizierter elektronischer Signatur und E-ID – zusätzliche *Liveness Detection* (Rz 38, 39, 44.3)

Stellungnahmen

Im Zusammenhang mit der Wohnsitzprüfung haben mehrere Anhörungsteilnehmende auf das erhöhte Fälschungsrisiko vor allem durch den Einsatz von KI-Werkzeugen sowie den Identitätsmissbrauch durch *Deepfake*-basierte Täuschungshandlungen hingewiesen. Um dieses Risiko zu reduzieren, schlugen sie vor, eine *Liveness Detection* (Lebenderkennung) als Ergänzung zur Wohnsitzprüfung vorzusehen.

Würdigung

Wie die FINMA in ihrer Aufsichtsmitteilung 02/2026 festhält, sind digitale Betrugsrisiken auch im Zusammenhang mit der digitalen Eröffnung von Kundenbeziehungen immanent. Im Hinblick auf die erwiesenermassen steigenden Risiken im Zusammenhang mit neuen Technologien scheint es deshalb sachgemäss, die bereits in Rz 32 vorgesehene *Liveness Detection* auch auf die weiteren Varianten der Online-Identifizierung zu adaptieren.

Das Sicherheitselement der *Liveness Detection* gilt im Markt als wirksames Mittel, um die Sicherheit bei Identifizierungsprozessen zu erhöhen und *Deepfakes* und KI-gestützte Fälschungen abzuwehren. Diese Einschätzung wurde im Rahmen der öffentlichen Anhörung in mehreren Eingaben bestätigt. Entsprechend erhöht die Kombination aus Wohnsitzprüfung und *Liveness Detection* das Sicherheitsniveau bei der Online-Identifizierung und adressiert die steigenden Betrugsrisiken.

Fazit

Das Erfordernis einer *Liveness Detection* wird in Rz 39 sowie 44.3 in Bezug auf die Online-Identifizierung mittels elektronischer Ausweiskopie mit QES und E-ID ergänzt.

3.3 Weitere Anliegen

3.3.1 Wirkung des Rundschreibens

Stellungnahmen

Ein Anhörungsteilnehmender brachte vor, dass Betrugsversuche im digitalen Bereich, insbesondere durch KI und Datenmissbrauch, zunehmend komplexer würden. Um die damit einhergehenden Risiken zu adressieren, seien die bestehenden Vorgaben des Rundschreibens regelmässig nicht ausreichend und müssten risikobasiert durch weitere Massnahmen ergänzt werden. Die FINMA solle deshalb klarstellen, dass das Rundschreiben Mindestvorgaben definiere, welche risikoabhängig zu ergänzen seien.

Würdigung

Die FINMA teilt die Auffassung, dass die Ausführungsbestimmungen des vorliegenden Rundschreibens als Mindestmass zu verstehen sind. Abhängig von der jeweiligen Risikolage und Geschäftsmodells des Finanzintermediärs können zusätzliche Sicherheitsmechanismen erforderlich sein. Trotzdem bedarf es keiner expliziten Klarstellung im Rundschreiben, zumal die im Rundschreiben definierte Praxis stets als Mindestmass zu verstehen ist und sich zusätzliche Sicherheitsmassnahmen insbesondere aus dem Erfordernis eines angemessenen Risikomanagements ergeben.

Fazit

Das Rundschreiben wird nicht angepasst.

3.3.2 Gleichstellung von elektronischen Identifizierungsnachweisen gemäss eIDAS-Verordnung

Stellungnahmen

Mehrere Anhörungsteilnehmende forderten eine gleichwertige Anerkennung von elektronischen Identifizierungsnachweisen, die von EU-Mitgliedstaaten gemäss der eIDAS-Verordnung ausgestellt wurden. Damit sollen regulatorische Barrieren und Medienbrüche im grenzüberschreitenden Kunden-*Onboarding* vermieden werden.

Würdigung

Die Berücksichtigung von elektronischen Identifizierungsnachweisen nach der eIDAS-Verordnung setzt eine technische sowie regulatorische Abstützung auf internationaler Ebene voraus. Während die eIDAS-Verordnung einen einheitlichen Rahmen für die EU-weite Anerkennung digitaler Identitäten

auf unterschiedlichen Vertrauensniveaus schafft, ist die Schweizer Lösung vorerst als nationales, staatsnahes System konzipiert und gesetzlich verankert. Eine Schweizer E-ID wird im Rechtsverkehr mit der EU nicht automatisch als gleichwertig anerkannt. Gleichermassen können elektronische Identifizierungsnachweise nach eIDAS nicht ohne weitere technische und regulatorische Prüfung in der Schweiz zur digitalen Identifizierung von Vertragsparteien nach diesem Rundschreiben zugelassen werden.

Fazit

Eine gleichwertige Anerkennung für nach der eIDAS-Verordnung ausgestellte elektronische Identifizierungsnachweise ist aktuell nicht vorgesehen.

3.3.3 Katalog von möglichen Identifizierungs- und Verifikationselementen

Stellungnahmen

Ein Anhörungsteilnehmer regte an, im Rundschreiben nicht die Details zur Video- und Online-Identifizierung zu regeln, sondern den Finanzintermediären einen nicht abschliessenden Katalog von möglichen Identifizierungs- und Verifikationselementen vorzugeben. Es solle dann letztlich dem Ermessen und in der Verantwortung der Finanzintermediäre überlassen werden, wie die GwG-Sorgfaltspflichten nach einem risikobasierten Ansatz erfüllt werden.

Würdigung

Die FINMA verfolgt zwar einen prinzipienbasierten und technologieneutralen Regulierungsansatz, der den Finanzintermediären ermöglicht, unterschiedliche technologische Lösungen zur digitalen Identifizierung von Vertragsparteien anzuwenden. Allerdings müssen die Anforderungen aus dem GwG und der GwV-FINMA in den digitalen Kontext übertragen werden. Zur Gewährleistung einer konsistenten Aufsichtspraxis sowie eines einheitlichen und hinreichenden Sicherheits- und Vertrauensniveaus zur Einhaltung der Vorgaben aus dem GwG sind deshalb aufsichtsrechtliche Minimalstandards erforderlich.

Fazit

Es wird auf einen nicht abschliessenden Katalog von möglichen Identifizierungs- und Verifikationselementen verzichtet

4 Weiteres Vorgehen

Das teilrevidierte FINMA-RS 16/7 tritt am 1. November 2026 in Kraft.

Für die Sicherstellung der Wohnsitzprüfung im Rahmen der Online-Identifizierung mittels QES gelten Übergangsfristen von einem Jahr ab Inkrafttreten.