SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Abs. SignD Identity GmbH
Gumpendorferstraße 83 / 1 / 1, 1060 Wien

Per email

Wien, 1.6.2021

Stellungnahme zu Novellierungsentwurf zur Online-Identitätsverordnung

Sehr geehrte Damen und Herren,

Im Zuge der sich laufend verbessernden Technologien und des unaufhaltsam wachsenden Bedarfs nach digitalisierten Onboardinglösungen ist es begrüßenswert, dass die FMA neue Wege ermöglichen will, wie der Finanzplatz Österreich attraktiver gemacht und die Verpflichteten mit besseren Möglichkeiten der Kundenindentifikation ausgestattet werden können. Wir denken jedoch, dass der aktuell vorgelegte Vorschlag zu kurz greift, im Gegensatz zu den wichtigsten Empfehlungen der EBA steht und den Sicherheitsaspekt ungenügend berücksichtigt.

Wir erlauben uns daher, folgenden Änderungsvorschlag einzubringen, der nicht nur Kundenerfahrung und Effizienz der Verpflichteten verbessern soll, sondern durch einen risikobasierten Ansatz und multiple Identifikationsfaktoren auch eine bessere Qualität ermöglicht.

Beste Grüße

Mirko Kinigadner – CEO Fonmony GmbH

Bernhard Reiterer – CEO Signd GmbH

Christian Pirkner – CEO Bluecode International GmbH

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Stellungnahme - Einleitung

Die Möglichkeit, moderne und sichere Verifizierungslösungen wie **NFC** und insbesondere die Validierung gegen die elektronische Ausweissignatur (Document Signer Certificate - **DSC**) sind jedenfalls begrüßenswert. Bereits vor COVID-19 war der Weg zur digitalisierten Begründung einer Geschäftsbeziehung der präferierte Weg großer Bevölkerungsgruppen und muss daher durch geeignete Methoden zur Fernidentifizierung unterstützt werden.

Allerdings befindet sich der österreichische Finanzmarkt bereits jetzt in einer benachteiligten Position durch die aktuell verfügbaren Möglichkeiten des FM-GWG im Vergleich zu anderen Staaten. Dieser Standortnachteil führt nachgewiesenermaßen zu regulatorischer Arbitrage von Unternehmen und mit zunehmender Digitalisierung auch Abwanderung der Österreicher selbst zu digitalen Angeboten, die aus anderen EU-Staaten mit zeitgemäßen und für den Konsumenten einfachen Methoden der Fernidentifizierung punkten. Der heutige Stand der Technik erlaubt es allerdings, geeignete, risikobasierte Methoden anzuwenden, die eine Identifikation für den Konsumenten einfach, aber gleichermaßen auch für Verpflichtete und in Folge den Regulator sicher und zuverlässig machen.

Der Vorschlag, NFC-basierte Identifizierungen für eine Fernidentifizierung einzusetzen ist gut, beinhaltet als alleinige Ergänzung allerdings etliche Risiken. Ein Fallback auf die anderen Legitimierungsmöglichkeiten des FM-GWG ist möglich, allerdings stellt sich hier dann auch die Frage, wieso die Online-Identifikationsverordnung nun überhaupt novelliert werden sollte, wenn sich hier keine signifikanten Verbesserungen für alle Beteiligten ergeben.

Die Finanzmarktaufsicht hat die einmalige Möglichkeit im Zuge dieser Novelle auch endlich den von der EBA und der EUR vorgegebene “risk-based approach” in die Regulierung einzuführen. EBA hat hierzu erst unlängst wieder in Ihrer Opion am 23.3.2021[1] hingewiesen. Wir sind selbst in engem Austausch mit EBA und denken, dass mittlerweile genug Länder bewiesen haben, dass der risikobasierte Ansatz einen Vorteil für den Finanzplatz, Erleichterungen für die Verpflichteten ohne Mehraufwand beim Regulator bedeutet. Wir empfehlen daher, den Standortnachteil nun in einen Vorteil umzukehren und die Verpflichteten mit zeitgemäßen Mitteln auszustatten, um auch zukünftig zu reüssieren und auch dem Regulator das Leben einfacher zu machen.

---

[1] EBA (EBA/Op/2021/04)

“33.Given the above, the EBA reminds CAs that they have to apply a risk-based approach to AML/CFT supervision under Article 48 of the AMLD. Furthermore, in line with Article 16 of the EBA’s founding Regulation, CAs have a legal duty to make every effort to comply with EBA’s Risk-based Supervision Guidelines. While these Guidelines are being updated, CAs are expected to have considered the recommendations set out in the EBA’s report on competent authorities’ approaches to the AML/CFT supervision of banks.”

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Änderungsvorschlag:

1. Dem § 4 wird folgender Abs. 6 angefügt:

„(6) Die Online-Identifikation kann auch durch geeignete Biometrische Identifikationsverfahren erfolgen. Dabei sind die Anforderungen dieser Verordnung nach Maßgabe der folgenden Bestimmungen einzuhalten:

1. Das Biometrische Identifikationsverfahren muss jedenfalls dem aktuellen Stand der Technik entsprechen, anlassbezogen aktualisiert werden und ein Sicherheitsniveau erreichen, mit dem zumindest eine der Online-Identifikation durch Mitarbeiter gleichwertige Erfüllung sichergestellt werden kann. Der Verpflichtete muss geeignete Maßnahmen zur Sicherung der Integrität und Sicherheit der verwendeten Verfahren treffen, einschließlich aktiver Überwachungsmaßnahmen, um etwaige Probleme unmittelbar zu erkennen und zu beseitigen.
2. Das Biometrische Identifikationsverfahren ist vom Verpflichteten nachvollziehbar zu dokumentieren. Abs. 2 erster Satz ist mit der Maßgabe anzuwenden, dass Aufnahmen, die zum Zwecke der Online-Identifikation erstellt werden, in ihrer Gesamtheit vom Verpflichteten akustisch und optisch aufzuzeichnen sind. Die Dokumentation umfasst jedenfalls auch die im Rahmen der Überprüfung herangezogenen Sicherheitsfaktoren und die Ergebnisse der einzelnen Prüfungsschritte.
3. Abs. 2 Z 2 und 3 ist mit der Maßgabe anzuwenden, dass anstelle der Anfertigung von Bildschirmkopien bei der Überprüfung elektronisch signierter Lichtbildausweise (Z 5) die elektronisch signierten Daten zu speichern sind.
4. Werden die Anforderungen gemäß Abs. 3 und 5 durch ein Biometrisches Identifikationsverfahren erfüllt, überprüft der Verpflichtete die tatsächliche Teilnahme des potentiellen Kunden oder seiner vertretungsbefugten natürlichen Person an der Online-Identifikation anhand geeigneter Sicherungsmaßnahmen, die jedenfalls die Überprüfung anhand einer während der Online- Identifikation erstellten Videoaufnahme umfassen (Liveness-Check). Der Liveness-Check kann von Abs. 3 Z 1 und 2 und Abs. 5 abweichen und ist vom Verpflichteten ~~akustisch und optisch~~ dem Verfahren nach mit allen Sicherheitsmerkmalen aufzuzeichnen und aufzubewahren.

~~5. Für Biometrische Identifikationsverfahren dürfen nur Lichtbildausweise, deren Inhalt von der ausstellenden Behörde elektronisch signiert worden ist, verwendet werden. Der Verpflichtete hat dabei die Echtheit der elektronischen Signatur des Lichtbildausweises und die Integrität der elektronisch signierten Daten zu überprüfen und sicherzustellen, dass zur Signatur kein kompromittierter Schlüssel verwendet worden ist. Im Rahmen des Biometrischen Identifikationsverfahrens hat der Verpflichtete auch eine Überprüfung der logischen Konsistenz gemäß Abs. 4 Z 5 vorzunehmen. Abs. 4 Z 1 bis 4 ist auf die Überprüfung der Authentizität des Lichtbildausweises im Rahmen eines Biometrischen Identifikationsverfahrens nicht anwendbar.“~~

Neuer Absatz 5.

5. der Verpflichtete eine geeignete Überprüfung des potenziellen Kunden oder der Geschäftsbeziehung unter Berücksichtigung der verfahrensbezogenen und risikobezogenen Anhaltspunkte das entsprechende Biometrische Identifikationsverfahren auszuwählen bzw. einzelne oder mehrere Identifikationsverfahren hinzuzunehmen welche den in § 4 Abs. 6 Z 1 bis 4 genannten verfahrensbezogenen Sicherungsmaßnahmen ergänzend sind.

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Stellungnahme – Kritische Auseinandersetzung

Die Identifizierung mittels NFC und biometrischem Abgleich hat große Vorteile, dahingehend dass im Vergleich zu einer optischen Identifizierung gesicherte Werte abgeglichen und mittels DSCs validiert werden können. Allerdings sind auch einige Nachteile hiermit verbunden.

Vorteile:

- Keine Lesefehler der Personen- und Ausweisdaten
- Extra Überprüfung Zertifikate

Nachteile:

- Optische Sicherheitsmerkmale können nicht mehr überprüft werden, hierbei fallen je nach Ausweistest bis zu 60 forensische Tests im Weißlicht aus
- bestehende Systeme und Prozesse passen nicht dazu (EBA rät, auf bestehende Prozesse Rücksicht zu nehmen).
- NFC benötigt zwingend eine native App. Die überwältigende Mehrheit der österreichischen Finanzinstitute haben ihre allerdings Antragsstrecken web- und nicht app-basiert. Gleichzeitig geht der Trend in der Bevölkerung gegen neue Individualapps, was die Akzeptanz und Bereitschaft verringert. Eine mobile Banking App mag noch argumentierbar sein, aber bei den meisten anderen Finanzdienstleistungen, wollen Nutzer nicht in eine App gezwungen werden.
- in manchen Ländern sind aktuell über 50% aller Zertifikate gültiger Reisepässe revoked. Das Dokument ist selbstverständlich weiterhin gültig, würde aber bei einer ordentlichen NFC-Identifizierung abgelehnt werden -> das führt zu Vorverurteilung und Einschüchterung der Kunden.
- Verbreitung biometrischer Chips hauptsächlich auf Reisepässen, nationale IDs erst seit 2021 EU-übergreifend. Eine volle Durchdringung ist für Ende 2031 (3.8.2031) zu erwarten.

Kritische Themen sind daher:

- Sicherheit NFC
- Gleichwertige Alternativen und Technologieneutralität
- Anwendbarkeit und Ausschluss von Bevölkerungsgruppen (Diskriminierung und Ausschluss durch De-Risking)
- Benachteiligung des Finanzplatzes und regulatory arbitrage
- Unvereinbarkeit mit EBA Empfehlungen (Avoidance of De-Risking, legacy process)

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Kritisches Thema 1: Sicherheit und gleichwertige Technologien

GESETZESVORSCHLAG

"Zu Z5: Biometrische Identifikationsverfahren müssen die Echtheit des Lichtbildausweises ab 1.April 2022 (§9 Abs.2) anhand der elektronischen Ausweissignatur überprüfen. Zur Überprüfung durch ein Auslesen der elektronisch gespeicherten Daten kommen insbesondere Reisepässe in Frage. Spätestens seit 2007 ist die Ausstellung biometrischer Reisepässe mit NFC-Chip international Standard. Auch die Verbreitung von NFC-fähigen Mobiltelefonen hat mittlerweile ein hohes Niveau erreicht. Daher bestehen keine hinreichenden Gründe mehr, um bei der biometrischen Identifikation neben der besonders fälschungssicheren Überprüfung anhand der elektronisch gespeicherten Daten auch eine weniger fälschungssichere, rein optische Überprüfung des Lichtbildausweises anhand einer vom Nutzer erstellten Bildaufnahme zuzulassen. Weiterhin zulässig bleibt die Überprüfung des Lichtbildausweises durch einen Mitarbeiter ohne Prüfung der elektronischen Signatur gemäß §4 Abs.4"

ANMERKUNG

Beim Validieren der Signaturen ist essentiell, die zugrundeliegenden Zertifikate in einer lückenlosen Überprüfung inklusive der sogenannten "Revocation" Listen durchzuführen. Das Vertrauen in die eingereichten DSC soll entweder durch Abgleich der DSC mit einer vertrauenswürdigen Liste von DSCs oder durch Aufbau einer Vertrauenskette zu einer vertrauenswürdigen Country Signing Certificate Authority (CSCA) und Überprüfung der DSC anhand einer Certificate Revocation List (CRL) erfolgen. Andernfalls ist von einer Scheinsicherheit ohne praktischen Wert auszugehen.

Wichtig ist auf die Einschränkungen und Limitierungen hinzuweisen. NFC funktioniert ausschließlich in nativen Applikationen - also nicht auf den momentanen Antragsstrecken der Finanzdienstleister, funktioniert auf absehbare Sicht nur mit europäischen Reisepässen bzw. einer erst jetzt langsam steigenden Anzahl an Personalausweisen und gibt keine verlässliche Auskunft über die Gültigkeit (sehr wohl aber die Authentizität) eines Ausweises.

Die Verordnung geht unserer Ansicht daher zu kurz, da hier ein großer Teil der in Österreich lebenden Bevölkerung und auch viele Finanzinstitute von einer Nutzung dieser Identifizierungslösung ausgeschlossen wird. Gleichzeitig besteht hier andererseits die Gefahr des de-riskings, indem hingenommen wird, dass Kunden aus ärmeren Schichten eine solche Technologie nicht verfügbar haben und hier eine automatische Negativselektion weniger rentabler Kunden erfolgt. Wir sehen vor allem auch die Gefahr, dass Kreditinstitute und andere Finanzdienstleister diese Möglichkeit der Diskriminierung auch in Präsenzsituationen auf diese Technologie stützen werden. Dieses wird die Diskriminierung und dadurch Ausschließung von Personen, welchen keine Europäischen Reisepass besitzen, weiter vorantreiben und beschleunigen. Da jedoch diese Personen auch Finanzdienstleistungen benötigen, werden diese Alternativen finden und benützen, was wiederum die Position des Regulators weiter schwächt.

Wir regen daher die zusätzliche Aufnahme weiterer, zeitgemäßer und ebenso sicherer Identifikationsalternativen als Stand der Technik an.

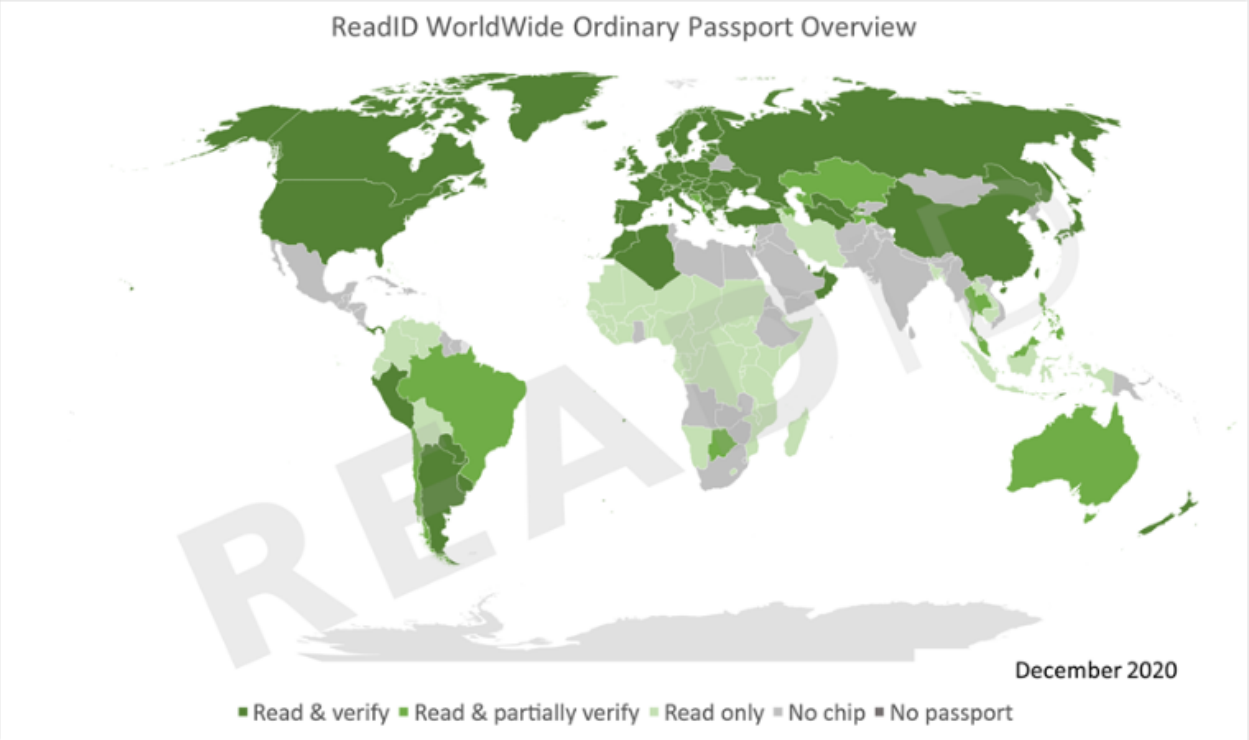
SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

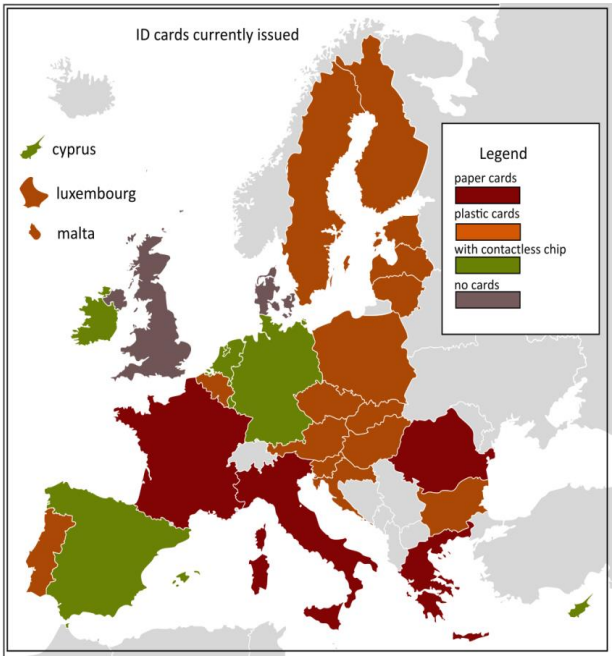
Kritisches Thema 2: Diskriminierung druch DE-RISKING

Diskriminerung und dadurch de-risking - insbesondere die unteren Schichten werden durch diese Regelung massiv in ihrem Zugang zum Finanzmarkt eingeschränkt (geringer Reisepass oder ID-Karten vorhanden). Viele Migranten (ca 17,1% der in Österreich lebenden Menschen) kommen aus Länder deren Reisepässe keinen biometrischen Chip haben (siehe Grafik unten). Europäische Personalausweise sind, wie in der Grafik auf der Folgeseite dargestellt, derzeit noch keine Alternative. Die europaweite Einführung von Chip-based ID-Karten startet erst mit August 2021 und wird bis August 2031 zum Umsetzen sein.

Anmerkung SignD: Aus der Praxis sei noch erwähnt, dass das bevorzugte Legitimierungsdokument des Österreichers der Führerschein ist. In hochvolumigen Situationen, etwa Mobilfunkanmeldungen, verzeichnen wir über 50% der Anmeldungen mit Führerscheinen und lediglich 30% mit Reisepässen.

Daher greift die Novelle zu kurz indem sie auf Funktionalität abstellt, die weder eine Verbreitung in der Bevölkerung hat, noch in den bestehenden Systemen der Verpflichteten einfach dargestellt werden kann, allerdings ein hohes Potential zum Ausschluss ganzer Bevölkerungsgruppen hat.





EBA hat in der letzten Opinion 23/3/2021 zu ML/TF diese Risiken explizit angesprochen:

“24. De-risking refers to a decision taken by firms to refuse, or to terminate, business relationship with some categories of customers that they associate with higher ML/TF risk. As explained in more detail in chapter 3.1.5. of the report, based on the responses received from CAs and the input received by the EBA in response to its Call for Input on de-risking,3the EBA notes that de-risking continues to pose ML/TF risks, because customers affected by de-risking may resort to alternative payment channels in the EU and elsewhere to meet their financial needs. As a result, transactions may no longer be monitored, making the detection and reporting of suspicious transactions and, ultimately, the prevention of ML/TF more difficult”

“25. In addition,a number of respondents to the EBA’s 2020 Call for Input suggested that de-risking is a practice that may be caused by firms failing to develop a sufficiently robust and comprehensive business-wide risk assessment and implement controls that effectively manage these risks. They also suggested that firms may choose not to manage the risk associated with individual business relationships and instead discontinuing business relationships with entire

categories of customers. As a result of this practice, certain individuals or entities may be excluded from the financial system.”

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Kritisches Thema 3: Zugang: “Risk Based”

Der aktuelle Vorschlag ignoriert die Vorgabe eines risikobasierten Ansatzes. EBA hat mehrfach klargestellt und berücksichtigt, dass Non-Face-to-Face nicht mehr als risikoreich angesehen werden. Der aktuelle Vorschlag erlaubt keine angemessene Methodenauswahl gemäß individuellem Kundenrisiko, Produktrisiko, Geschäftsmodell oder technologischem Stand des Unternehmens oder der Branche. Ziffer 5 soll vielmehr das Kriterium der größtmöglichen Risikoreduzierung anstreben, obwohl in vielen Anwendungsgebieten hier überbordende Maßnahmen gesetzt werden und das Risiko tatsächlich nicht ausreichend berücksichtigt wird – Stichwort: Scheinsicherheit.

In Anbetracht des Ansatzes des aktuellen Vorschlags werden auch Finanzdienstleister, die traditionell kleinere Kundenstöcke auch über die Entfernung verwalten (zB Vermögensberater) oder solche auf "gelegentliche Transaktionen" angewiesen sind, ganze Kundengruppen ausschließen müssen. Gleichermaßen werden auch im normalen Banking für nicht-kritische Geschäftsbeziehungen dieselben Identifikationshürden auferlegt wie bei geldwäscheanfälligen Services.

EBA warnt explizit und wiederholt vor dieser Gefahr:

EBA in ihrer Stellungnahme (EBA/Op/2021/04)

“ 26.Given the above, the EBA proposes that CAs remind the firms under their supervision that the EBA’s Risk Factors Guidelines4are clear that the application of a risk-based approach does not require firms to refuse or terminate business relationships with entire categories of customers that are considered to present high ML/TF risk, as the risk associated with individual business relationships may vary, even within one category. The guidelines set out factors that firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction and explain the need to carefully balance financial inclusion with the need to mitigate ML/TF risk. As regards the specific issue of corresponding banking relationships, the guidelines furthermore provide detailed guidance to help firms comply with their obligations under the AMLD in an effective and proportionate way.”

EBA’s Risk Factors Guidelines4 04/01/2018

Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence:

‘Risk-based approach’ means an approach whereby competent authorities and firms identify, assess and understand the ML/TF risks to which firms are exposed and take AML/CFT measures that are proportionate to those risks.

Firms should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one category.”

As example for money remitter the EBA states:

"133. The following factor may contribute to reducing risk: the funds used in the transfer come from an account held in the payer's name at an EEA credit or financial institution."

135. The following factors may contribute to reducing risk:
- The customer is a long-standing customer of the firm whose past behaviour has not given rise to suspicion and there are no indications that the ML/TF risk might be increased.
- The amount transferred is low; however, firms should note that low amounts alone will not be enough to discount TF risk.

Further the EBA writes in its opinion (JC 2017 81)

"Furthermore, EU law no longer designates situations where a customer is not physically present for identification purposes as high risk in all cases. Instead, Annex III to Directive (EU) 2015/849 lists non-face-to-face business relationships or transactions 'without certain safeguards' as 'potentially higher risk' in recognition of approaches to non-face-to-face verification of identity becoming more reliable.

12. However, since Directive (EU) 2015/849 lays down only minimum CDD requirements that firms must comply with, Member States have some flexibility in imposing more stringent standards through their national legislation where this is necessary in the light of the ML/TF risk."

Kritisches Thema 4: Technologieneutralität und -fortschritt:

EBA fordert, dass innovative Systeme sich in bestehende Workflows und Legacysysteme einbetten können müssen. Die Mehrzahl aller Finanzinstitute haben ausschließlich webbasierte und keine App-basierten Anmeldestrecken, selbst wenn sie Mobile Banking Apps anbieten. Viele Services sind sogar ausnahmslos über Web erreichbar. Es gilt auch zu beachten, dass mobile banking Angebote aktuell immer noch einen kleinen, wenn auch schnell wachsender Teil der online Konten darstellen.

Ein erzwungener app-basierter Ansatz ist auch nicht mehr zeitgemäß, da der Trend weg von Individualapps geht. NFC ist aber ausschließlich in nativen Apps oder SDKs möglich. Aktuell gibt es keine einzige technische Alternative, um NFC außerhalb nativer Apps oder über das Smartphonebetriebssystem für diese Zwecke zu verwenden. Im Crypto Bereich aber auch im Banking in anderen Ländern werden Identifizierungen mittlerweile bequem über den “channel-of-choice” des Konsumenten angeboten, teilweise sogar über Whatsapp oder Telegram. Der Stand der Technik erlaubt es, Identifizierungen in solchen Kanälen mit derselben Sicherheit auszugestalten. Nutzer werden die Services nutzen, die ihren Gewohnheiten entsprechen. Wenn österreichische Finanzinstitute, das nicht schaffen oder dürfen, werden Nutzer einfach woanders hin abwandern.

Ein Blick auf den Markt

Aktuell gibt es mit einer Ausnahme, die im Juni startet, ausschließlich nicht-österreichische Banken, die die Antragsstrecke innerhalb einer nativen App anbieten. Derzeit müssten 100% der österreichischen Finanzdienstleister ihr Serviceangebot ohne wirtschaftliche Begründung massiv umstellen.

EBA (JC 2017 81)

“With regard to innovative solutions for ongoing monitoring purposes, are controls in place to ensure that innovative solutions are operating effectively and efficiently? The ESAs consider it pertinent for the competent authorities to ensure that firms have considered the following factors:

Can the innovative solution be integrated with **firms’ existing workflows and legacy systems**? The ESAs believe that the innovative solution should be fully integrated with current and legacy systems used by firms and should have full access to all available information on their customers across multiple accounts (current and historical) and networks.”

SignD Identity GmbH
Gumpendorferstraße 83/1/1
1060 Wien
www.signd.id

Kritisches Thema 1: Scheinsicherheit

NOVELLENVORSCHLAG - Z2 (§4 Abs.3 Z2):

Auch bei der gewöhnlichen Online-Identifikation durch einen Mitarbeiter des Verpflichteten ist es künftig möglich, dass der Kunde anstelle der Seriennummer seines Lichtbildausweises eine vom Verpflichteten zufällig generierte, zumindest achtstelligeZeichen-oder Wortfolge vorliest. Damit werden die Anforderungen an die Online-Identifikation an die Anforderungen an den Liveness-Check im Rahmen einer Biometrischen Identifikation angenähert (Abs.6 Z4). Als Zeichenfolge gilt auch eine Ziffernfolge.

ANMERKUNG

Wir begrüßen den Vorstoße eine starke Lebenderkennung durch Zusatzschritte zu konstruieren, denken aber, dass andere Verfahren ebenbürtig oder zielgerichteter sind. Wir schlagen vor, statt der ausschließlichen Verwendung der mittlerweile in die Jahre gekommenen gestenbasierten Verfahren in Kombination mit zusätzlichen Nutzerhürden, auch moderne und überlegene System verwendbar zu machen.

Lebenderkennung:

Gestenbasierte Lebenderkennungen sind die älteste Form der Lebenderkennung und haben ihre Sicherheitsmöglichkeiten bereits ausgereizt. Das Hinzufügen zusätzlicher Challenges, etwa pass phrases bringt nur geringen Sicherheitsgewinn oder gar keinen bei Relaying oder Deep Fake.

Moderne Systeme verwenden schwierig zu überlistende Systeme wie passive Lebenderkennung und Genuine Presence Control.

Auch hier wird ein risikobasierter Ansatz gefordert, den die österreichische Regelung nicht berücksichtigt, da sie direkt auf den erweiterte Sorgfaltspflicht abstellt.

EBA in ihrer 23.Jan.2018 Opinion:

"15. In the ESAs' view, competent authorities should consider a number of factors when assessing the extent to which the use or intended use of **innovative CDD solutions is adequate in the light of the ML/TF risk associated with individual business relationships and firms' business-wide risk profiles**. These factors are technology-neutral and apply in addition to the customer, product, services, transaction, delivery channel and geographical risk factors firms should consider when assessing the risks associated with their business relationships, in line with Article 8 of Directive (EU) 2015/849 and Risk Factors Guidelines10. In particular, competent authorities should consider:

- oversight and control mechanisms;
- the quality and adequacy of CDD measures;
- the reliability of CDD measures;
- delivery channel risks; and
- geographical risks."

"Is there a risk that the customer's image visible on the screen is being tampered with during the transmission? The ESAs believe that competent authorities should ensure that firms have sufficiently robust controls in place to prevent or reduce such risk. These controls may include **some or all** of the following:

- feature whereby a customer is required to have a live chat with an administrator who has received specialised training in how to identify possible suspicious or unusual behaviour or image inconsistencies;
- built-in computer application that automatically identifies and verifies a person from a digital image or a video source (e.g. biometric facial recognition);
- requirement for a screen to be adequately illuminated when taking a person's photograph or recording a video during the identity verification process;
- built-in security feature that can detect images that are or have been tampered with (e.g. facial morphing) whereby such images appear pixelated or blurred.

The ESAs believe that firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include **one or more** of the following:

- built-in features which enable them to detect fraudulent documents on the basis of the documents' security features (i.e. watermarks, biographical data, photographs, lamination, UV-sensitive ink lines) and the location of various elements in the document (i.e. optical character recognition);
- features that compare the security features ingrained in the identity document presented during the transmission with a template of the same document held in the firms' internal identity document database;
- limiting the type of acceptable identity documents to those that contain: high security features or biometric data including finger prints and a facial image (e.g. e-passports and e-ID);

VORSCHLÄGE - Erklärung

Trotz aller Vorteile von NFC-basierten Verfahren, stellt ein ausschließlicher Fokus darauf eine massive Beeinträchtigung der Wettbewerbsfähigkeit der österreichischen Finanzwelt dar und birgt die Gefahr der Ausgrenzung von ganzen Kundengruppen.

Um ihre Services anbieten zu können, sind Finanzinstitute gezwungen, erfolgreiche Anmeldesysteme oder ihr gesamtes Servicespektrum (Webprozess muss plötzlich in eine App gegossen werden) oder es werden massive Medienbrüche in Kauf genommen (Download einer Identitätsapp -> noch mehr Abbrüche und Abwanderung von Instituten und innovativen Neugründungen in Ländern mit risikobasierten Identifikationsregularien).

Zusätzlich werden große Gruppen der Bevölkerung ausgeschlossen, da sie keinen Chip-inkludierten Reisepass haben.

Es ist vielmehr ein risikobasierter Ansatz anzustreben, bei dem gemäß der Risikoklasse des Kunden jeweils passende Sorgfaltspflichten angewendet werden können. Im Sinne der Technologieneutralität müssen auch alternative Lösungen zu NFC (zB optische Dokumentenverifizierung mit anderen Sicherheitsmerkmalen), die nachgewiesenermaßen gleich sicher sind, akzeptiert werden.

Anzumerken ist auch, dass mehrstufige Identifikationsprozesse einem einstufigen immer überlegen sind. Das gilt auch für die NFC-Identifizierung. Daher sind auch über die NFC Überprüfung und Lebenderkennung hinaus weitere Sicherungsschritte unbedingt zu empfehlen. Bei der NFC-Identifizierung werden etwa die meisten der Sicherungsmerkmale eines Ausweises nicht überprüft, somit sind MRZ+Chip Fakes äußerst einfach in der Lage, eine reine NFC Identifizierung zu überlisten. Als Abhilfe kommen hier Adressverifizierungen und Mobilfunkdaten oder eine risikobasierte Sicht in Frage. Die Sicherungsvorschläge mittels gestenbasierter Lebenderkennung und einzelner OTP-Phrasen sind gute Ansatzpunkte, doch nicht ausreichend, da diese mittels replay oder deek-fake überlistet werden können. Diese Schwachstellen können durch bessere Ausweisverifizierung, bessere Lebenderkennungssysteme und vor allem durch Hinzufügen kleiner zusätzlicher Verifizierungsschritte ausgemerzt werden, ohne die User Experience durch Pass Phrases und One Time Passwords mit Medienbruch zu verschlechtern und zu ähnlich schlechten Nutzungsraten wie bei der Videoidentifizierung zu führen.

Unsere Vorschläge sind neben einer simplen Erweiterung durch NFC-Identifizierung, zusätzliche Möglichkeiten je nach “Stand der Technik” im Zuge eines risikobasierten Ansatzes und einem Transaktionsmonitoring zu erweitern. In anderen Ländern erprobte Varianten sind etwa:

Verbesserte Referenzüberweisung:

- Photoidentifizierung - eine Photoidentifizierung kann durch Verwendung bestimmter Services leicht auf das Sicherheitsniveau einer NFC Identifizierung gebracht werden. Es gibt zugegebenermaßen nur wenige Services, die verlässlich die optischen Sicherheitsmerkmale sicher verifizieren können.
  (Ausweisverifizierung und Fälschungserkennung durch Analyse aller mit einer Smartphonekamera verwertbaren Sicherheitsmerkmale biometrischer Abgleich und Lebenderkennung mit sichereren Verfahren als den gestenbasierten.
  !*Diese Variante sollte im Hochrisikobereich zumindestens immer auch als Ergänzung zur NFC-Identifizierung angewendet werden!*
- Adressverifizierung (programmatische Überprüfung, ob eine Person tatsächlich an einer Adresse wohnt)
- PSD2-Login mit Account Information Service (Als Ersatz der Referenzüberweisung, die keinerlei Mehrwert in der Feststellung des Kontoinhabers hat bzw weniger Aussagekraft als das real-time-login)

Gehärtete Photoidentifizierung:

- Photoidentifizierung, aber zusätzlich weitere Sicherungsmaßnahmen, etwa:
- Mobile Identification (zumindest Name, Mobilfunknummer, Nationalität und aktueller Besitz des Geräts)
- Gegebenenfalls risikobasiert ergänzt durch:
  - Adressverifizierung
  - Überprüfung gegen Account Takeover und anderer Risikofaktoren

Risikobasierte sichere Photoidentifizierung:

Für low-risk Situationen, etwa einfache Kontoeröffnungen, und hinsichtlich des Novellenpunkts: *“Weiterhin zulässig bleibt die Überprüfung des Lichtbildausweises durch einen Mitarbeiter ohne Prüfung der elektronischen Signatur gemäß §4 Abs.4”*

Eine Photoidentifizierung (manchmal auch mit der von IDNow vermarkteten Lösung “Autoident” verwechselt) ist nachgewiesenermaßen einer Begutachtung durch geschulte Personen überlegen und kann nicht ermüden. Wir unterstützen diese Aussage und sind schlagen vor, eine automatisierte Variante der Personalsichtung für risikoarme Situation als ausreichend zu erachten.

Auch wollten wir noch einmal hervorheben, dass die EBA klar gegen eine Einschränkung auf bestimmte Technologien hinweist in ihrer Opinion “innovative solutions” (JC 2017 81).

Weiterführende Informationen

Exkurs:

The term **Liveness Detection** describes the ability of an AI-based biometrics recognition system to recognize the differences between a physically present human being and an inanimate spoof artifact. In high-risk use cases, Liveness Detection is a required step of a Photo Identification or Video Identification process.

Generally, there are two approaches to Liveness Detection:

- **Active Liveness Detection**: requires active participation by the customer through gestures like nodding or blinking. This is the older method for Liveness Detection and can be fooled by several strategies.
- **Passive Liveness Detection**: requires no participation by the customer, but makes use of the device camera. There are several approaches to ascertaining liveness in a passive way, like flashing lights at the customer or taking a video.

Generally speaking, Passive Liveness Detection is considered to be safer than Active Liveness Detection. However, in some use industries Active Liveness Detection is required by regulation and cannot be substituted by a passive approach. Regardless of approach, Liveness Detection data must not be saved, as Liveness Detection has to be repeated for each instance of authentication.

Genuine Presence Assurance is a method for passive Liveness Detection. This method prevents fraud through deepfakes by sending light signals through the device screen.

The process is secure and customer friendly, since the selfie is taken automatically and then converted to a canny image, a line drawing of the customer's face which includes all markers of their facial geometry. As a result, this product prevents triggering Selfie Anxiety within the customer.

Most available passive liveness detection solutions have been able to avoid any breaches so far.