Stellungnahme

der

IDnow.

im Rahmen des

Referentenentwurfs des Bundesministeriums der Finanzen (BMF) zur

Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung

(Geldwäsche Videoidentifizierungsverordnung - GwG VideoIdent)

(Bearbeitungsstand: 20.03.2024)

Stand: 16.05.2024

Inhaltsverzeichnis

1. Einführung

Die IDnow GmbH dankt dem Bundesministerium der Finanzen (BMF) und dem Bundesministerium des Innern (BMI) für die Möglichkeit, am Konsultationsverfahren teilzunehmen, das im Rahmen des Entwurfs der Rechtsverordnung zur Geldwäscheerkennung durch Videoidentifizierung (GwVideoIdentV) eingeleitet wurde.

IDnow ist ein führender Anbieter von Identifizierungslösungen in Deutschland und Europa. Unser umfassendes Portfolio an Identifizierungsverfahren bedient derzeit mehr als ein Drittel des deutschen Marktes im regulierten Anti-Geldwäsche (AML)-Umfeld. Seit unserer Gründung im Jahr 2014 bieten wir ein breites Spektrum an Identifizierungsverfahren an, darunter Kurier- und Filialverfahren, Video- und KI-basierte Verfahren, die Online-Identifizierungsfunktion des deutschen Personalausweises ("eID") sowie in diesem Jahr auch qualifizierte Vertrauensdienste und eine Wallet. Unsere fortschrittliche Identity-as-a-Service-Plattform verifiziert jährlich die Identitäten von mehr als 35 Millionen Menschen aus fast 195 verschiedenen Ländern in Echtzeit. Zahlreiche deutsche Branchenführer wie Commerzbank, Solarisbank, Teambank und die Sparkassen vertrauen auf unsere Verifikationslösungen.

Vor diesem Hintergrund begrüßen wir den vorgelegten Referentenentwurf zur Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung. Wir sind der Ansicht, dass neue Regelungen für teil- und vollautomatisierte Verifizierungslösungen gleiche Wettbewerbsbedingungen schaffen und die notwendige Struktur für einen sicheren Identitätsnachweis bieten können. Dies trägt dazu bei, robuste Sicherheitsstandards zu erreichen und das Vertrauen in digitale Dienste zu stärken. Wir begrüßen ebenfalls die eID zu fördern, da die eID aus unserer Erfahrung ein sicheres, zuverlässiges, benutzerfreundliches und kosteneffizientes Mittel zur Identifizierung ist.

Dank unserer langjährigen Erfahrung und der daraus gewonnenen Erkenntnisse sind wir zuversichtlich, einen wertvollen Beitrag zu dem Verordnungsentwurf leisten zu können. Der derzeitige Entwurfsstand gefährdet aus unserer Sicht die Wettbewerbsposition Deutschlands im Bank- und Finanzwesen sowie in anderen Branchen, die auf Identitätsprüfungen und Vertragsabschlüsse angewiesen sind. Insbesondere die Anforderungen in den Abschnitten §§ 10 und 11 werden die Marktposition des deutschen Bankensektors sowohl im Inland als auch international verschlechtern. IDnow begrüßt die Gelegenheit, seine Erfahrungen und seinen umfangreichen Datenbestand zur Verfügung zu stellen, um beizutragen, dass die vorgeschlagenen Änderungen ausreichend sicher und benutzerfreundlich bleiben und einen wettbewerbsfähigen deutschen Markt fördern.

Basierend auf unserer Erfahrung ist es entscheidend, dass der deutsche Markt den Nutzern verschiedene Identifizierungsmethoden im Sinne der Technologieneutralität zur Auswahl stellt. Der GwVideoIdentV-E sollte die Wahlmöglichkeiten der Nutzer nicht so einschränken, dass bestimmte Nutzergruppen vom Verfahren ausgeschlossen und dadurch diskriminiert werden. Die GwVideoIdentV sollte eine Grundlage für marktgerechte, nachhaltige und zukunftssichere Identifizierungslösungen schaffen. Die Verpflichteten sollten in der Lage sein, verschiedene Verfahren anzubieten, wie es in § 12 Absatz 1 des GwG vorgesehen ist. Bei IDnow ist dies bereits der Fall: Wir bieten unseren Kunden und Endnutzern die Möglichkeit, sich mit der eID zu identifizieren, und ermöglichen zudem die Nutzung anderer Verfahren wie VideoIdent.

Darüber hinaus fördert die Technologieneutralität bedeutende Beiträge der deutschen Forschung und Entwicklung im Bereich der Identitätsüberprüfung. IDnow setzt durch seine Beiträge zu Standardisierungsorganisationen wie dem Europäischen Telekommunikationsinstitut (ETSI), dem Europäischen Komitee für Normung (CEN) und der Europäischen Agentur für Cybersicherheit (ENISA) immer wieder Maßstäbe für Sicherheitsstandards. Unsere Beiträge zu Verifizierungs- und Authentifizierungsprozessen unterstützen die Neuerungen von Standards, die als technische Grundlage für die Durchführungsbestimmungen der eIDAS2-Verordnung dienen.

2. Förderung der eID

IDnow unterstützt explizit das Ziel, die eID als eine Methode für AML-Anwendungsfälle zu fördern, da die eID ein sicheres, zuverlässiges, benutzerfreundliches und kosteneffizientes Mittel zur Identifizierung ist.

Aktuell setzen viele Banken die eID noch nicht ein. Bei den deutschen Kunden im Bank- und Finanzwesen von IDnow liegt die Nutzung der eID derzeit bei etwa 1,5 %. Bei den Kunden, die die eID nutzen, sehen wir eine durchschnittliche Nutzungsrate von 15 %. Dies zeigt, dass viele Kunden die eID noch nicht anbieten, obwohl wir bereits mehrere Marketingkampagnen für die eID durchgeführt haben.

Insgesamt ist festzuhalten, dass die eID noch weit davon entfernt ist, ein flächendeckendes Verfahren zu sein. Gleichzeitig nutzen etwa 65 % unserer deutschen Kunden den deutschen Personalausweis. Auch die verbleibenden 35 % müssen zukünftig die Möglichkeit haben, sich sicher und digital zu identifizieren. Eine Rückkehr zur persönlichen Identifizierung würde der Digitalisierung in Deutschland nachhaltigen Schaden zufügen.

IDnow ersucht um Klärung und Berücksichtigung der folgenden Empfehlungen:

Die Anforderung, die eID sowohl für eine halbautomatisierte als auch für eine vollautomatisierte Lösung anzubieten, sollte präzisiert werden. In der aktuellen Formulierung wäre die eID nur für ein video- und halbautomatisiertes Verfahren erforderlich, was nicht dem Sinn der Verordnung entsprechen kann.

Formulierungsvorschlag

§ 5(2): Das Videoidentifizierungsverfahren und das teilautomatisierte **sowie das vollautomatisierte** Videoidentifizierungs-verfahren dürfen nur verwendet werden, wenn der Verpflichtete für diesen (…)

§ 5 schreibt vor, dass die Verpflichteten über ein Verfahren verfügen müssen, das die deutsche eID "in gleichwertiger Weise" zu anderen Lösungen anbietet. Grundsätzlich begrüßen wir dies. Unser Ansatz würde jedoch noch weiter gehen: Wir würden zuerst die eID versuchen und, falls dies nicht erfolgreich

ist, VideoIdent verwenden. Wir empfehlen, "mindestens in gleichwertiger Art und Weise" einzufügen, um zu betonen, dass die eID als erstes Identifikationsverfahren angeboten werden soll.

Formulierungsvorschlag

§ 5(2): (…), wenn der Verpflichtete für diesen Identifizierungsvorgang **mindestens** in gleichwertiger Art und Weise auch ein Verfahren zur Überprüfung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anbietet.

Zudem muss festgestellt werden, dass die eID nur angeboten werden kann, sofern dies überhaupt möglich ist. Wenn sich also eine Person mit einem ausländischen Ausweisdokument oder einem deutschen Reisepass identifizieren will, gibt es keine Möglichkeit die eID zu nutzen.

Formulierungsvorschlag

§ 5(2): (…) auch ein Verfahren zur Überprüfung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anbietet **sofern die Nutzung des elektronischen Identitätsnachweises durch den Nutzer bei diesem Vorgang möglich ist.**

Die eID ist ein sicheres, zuverlässiges und schnelles Verfahren. Sie wird als Grundlage für die deutsche Umsetzung der EUDI-Wallet dienen und sollte daher breite Akzeptanz in der Bevölkerung genießen. Es sollte jedoch bedacht werden, dass die Verpflichtung, die eID für jeden Anwendungsweg bei Banken, in dem das Video-Identifikationsverfahren zum Einsatz kommt, anzubieten, möglicherweise nicht ausreichend ist, um die Nutzerakzeptanz für eine zukünftige EUDI-Wallet in dieser kurzen Zeit zu erhöhen. Wir würden es begrüßen, wenn der Austausch mit dem privaten Sektor fortgesetzt würde, um Ideen zu entwickeln, wie die eID durch zusätzliche Maßnahmen bekannt gemacht und weiter verbreitet werden kann.

3. Geeignete Ausweisdokumente (§ 10) und Überprüfung der zu identifizierende Person (§ 11)

Die in den Absätzen 10 und 11 genannten Anforderungen hätten erhebliche Auswirkungen auf die Identifizierungsverfahren mit schädlichen Folgen für den Banken- und Finanzsektor. Diese Abschnitte schränken die Anzahl der Identitätsdokumente, die anhand dieser neuen Kriterien überprüft werden können, drastisch ein. Würden die Anforderungen des § 10 durchgesetzt, wären etwa 75 % der Identifikationsdokumente, die IDnow für sein VideoIdent-Verfahren nach dem aktuellen Rundschreiben 3/2017 verwendet, effektiv ausgeschlossen.

Im Jahr 2023 wurden 35 % unserer Kundenidentifikationen im deutschen Finanzsektor mit dem deutschen Reisepass oder mit ausländischen (EU und nicht-EU) Dokumenten durchgeführt. Auf der Grundlage dieser Statistiken würde die Verordnung die Marktdominanz der deutschen Banken beim Angebot von Dienstleistungen und Produkten sowohl im Inland als auch im Ausland erheblich beeinträchtigen.

Untenstehend möchten wir exemplarisch auf die Auswirkungen von § 10 hinweisen:

- Die Anforderung, dass das ID-Dokument mindestens eine beugungsoptisch wirksame Struktur im Fotobereich enthalten muss, würde fast 19 Prozent der derzeit von IDnow verwendeten ID-Dokumente ausschließen.[1]
- Die Anforderung, dass „mindestens eine Prägung im Bereich individueller Eintragungen oder mindestens eine taktile individuelle Eintragung“ vorhanden sein muss, würde 52 Prozent der derzeit von IDnow identifizierten Ausweisdokumente ausschließen, darunter auch deutsche Ausweisdokumente.
- Die Anforderung, dass mindestens ein Sekundärlichtbild enthalten sein muss, würde 26 Prozent der von IDnow genutzten Ausweisdokumente ausschließen.

Diese Änderungen betreffen auch Dokumente der neuesten Generation aus anderen Ländern, die unserer Erfahrung nach hochsicher sind und sehr geringe Betrugsraten aufweisen.

[1] Die Daten basieren auf internen IDnow-Identifikationen für VideoIdent in Deutschland.

Zudem würden die noch strengeren Anforderungen an die Prüfung geeigneter Ausweisdokumente (§ 11) auch deutsche Ausweisdokumente betreffen, sodass auch diese praktisch nicht mehr prüfbar wären.

Untenstehend möchten wir exemplarisch auf die Auswirkungen von § 11 hinweisen:

- Die Anforderung, dass vorhandene Sekundärlichtbilder mit den anderen Fotos abgeglichen werden müssen, ist praktisch nicht erfüllbar. Sekundärlichtbilder sind oft zu klein, zu ungenau oder nicht vollständig sichtbar. Auch deutsche Ausweisdokumente sind davon betroffen (siehe Anhang I).
- Es ist nicht klar, wie die physische Oberfläche des Dokuments bei einer Videoidentifizierung ohne Berührung des Dokuments überprüft werden kann.
- Auch die Forderung, dass alle in Sicherheitsmerkmalen integrierten Individualdaten mit den in der Sichtzone integrierten Daten abgeglichen und auf Echtheit geprüft werden müssen, ist praktisch nicht erfüllbar. Viele dieser Daten in Sicherheitsmerkmalen sind zu klein oder nicht vollständig sichtbar. Auch deutsche Ausweisdokumente sind davon betroffen (siehe Anhang I).
- Die Kategorisierung der Sicherheitsmerkmale erscheint uneinheitlich und unvollständig. Zum Beispiel enthält das Identigramm (Kategorie 1) auch Personalisierungstechnologie (Kategorie 2). Einige Merkmale, insbesondere von ausländischen Identitätsdokumenten, sind nicht mehr aufgeführt. Die Reduzierung der Anzahl der Sicherheitsmerkmale macht eine zufällige Auswahl der zu prüfenden Merkmale in vielen Fällen praktisch unmöglich, insbesondere in Kategorie 3.
- Die Durchführung der in § 11 geforderten Maßnahmen ist selbst in einer physischen Umgebung praktisch unmöglich und wird nach unserem Wissen nicht einmal bei Polizeikontrollen durchgeführt. Außerhalb von speziellen Laborbedingungen, wie beispielsweise beim BKA, sind diese Anforderungen praktisch nicht zu erfüllen.
- Die Auswirkungen der §§ 10 und 11 betreffen nicht nur die Identifizierung deutscher Ausweisdokumente, sondern auch eine erhebliche Anzahl ausländischer Ausweise. Ausländische Einwohner oder Personen mit Wohnsitz im Ausland, die einen ausländischen Personalausweis besitzen, könnten mit einer deutschen Lösung nicht mehr identifiziert werden. So wären beispielsweise österreichische, niederländische und französische Pässe, die über ausreichende Sicherheitsmerkmale verfügen, für ein deutsches Videoverfahren nicht mehr zulässig.

Marktverzerrung im Vergleich zu anderen Ländern

In Frankreich hat sich die französische Bankenaufsicht (ACPR) an ihre Cybersicherheitsagentur ANSSI (entspricht dem deutschen BSI) gewandt, um einen neuen Standard für die Identitätsüberprüfung zu definieren, der als "Prestataire de Vérification d'Identité à Distance" (PVID) bekannt ist. Diese Norm umfasst technische und betriebliche Anforderungen, die Diensteanbieter erfüllen müssen, um von der ANSSI anerkannt zu werden.

Die Liste, der im Rahmen des PVID zugelassenen Identitätsdokumente, ist umfangreich und basiert auf den Kriterien der PRADO- und ICAO-Normen. Nationale und gebietsansässige Personalausweise aus Frankreich und anderen europäischen Mitgliedstaaten, einschließlich des EWR und der Schweiz, sowie Reisepässe enthalten Kriterien und Merkmale wie:

- Material, das entweder integriert oder laminiert ist
- Mindestprüfungen aus einer Reihe von Sicherheitsmerkmalen aus verschiedenen Kategorien
- Fotoschutz
- Biometrische Fotoqualität
- Ausreichende Datenfelder mit maschinenlesbarer Zone (MRZ) + Sichtbereich + Sicherheitsmerkmale
- *Checksums* sollten verfügbar sein

In Anhang II ist die aktuell akzeptierte Liste nach PVID aufgeführt. Diese Dokumente wurde von der ANSSI in Zusammenarbeit mit der nationalen Polizei in Frankreich offiziell geprüft und für sicher befunden.

Wie aus dem Anhang ersichtlich, sind dort viele Dokumente zugelassen, die nach den neuen Anforderungen aus §§ 10 und 11 nicht mehr zugelassen wären.

Wie bereits erwähnt, würde dies in Deutschland zu erheblichen Marktverzerrungen führen. Deutsche Banken und Fintechs stehen im Wettbewerb mit ausländischen Banken, um ausgewählte Produkte und Dienstleistungen digital im In- und Ausland anzubieten. Banken in anderen EU-Ländern können deutsche Bürger problemlos einbinden, da ihre Verfahren aktuelle und neue Ausweisdokumente digital akzeptieren. Die Wettbewerbsposition Deutschlands zu schwächen, ist sicherlich nicht das Ziel des Referentenentwurfs.

Schließlich soll die EU-Geldwäscheverordnung noch in diesem Jahr verabschiedet werden und bis 2027 mit definierten Know-Your-Customer (KYC) Onboarding-Prozessen in Kraft treten. Angesichts der

vorgeschlagenen Änderungen in §§ 10 und 11 und unter Berücksichtigung der neuen AMLR empfiehlt IDnow dem BMF/BMI, die Anforderungen an geeignete Ausweisdokumente aus dem bestehenden BaFin-Rundschreiben 3/2017 beizubehalten. Diese haben sich als praxistauglich und ausreichend sicher erwiesen und stellen eine diskriminierungsfreie Grundlage zur Überprüfung jeglicher Ausweisdokumente dar. Gleichzeitig sind die aktuellen Anforderungen im Arbeitskreis Fernidentifizierung gemeinsam mit dem BMI, BSI und BKA erarbeitet worden und erfüllen aus unserer Sicht weiterhin gut ihre Zwecke.

4. Arbeitskreis Fernidentifzierung

Eine Wiederaufnahme des Arbeitskreises Fernidentifizierung, der erstmals 2016 ins Leben gerufen wurde, würden wir sehr begrüßen. Der AK profitierte von dem wertvollen Austausch zwischen den beteiligten Ministerien, Vertretern der Finanzbranche und Identifizierungsdienstleistern. Als Resultat wurde das BaFin Rundschreiben 3/2017 erstellt, das sich als überaus nützlich und anwendungsfreundlich erwiesen hat, während es die höchsten Sicherheitsstandards beibehielt.

Wir schlagen vor, den Arbeitskreis Fernidentifizierung wieder zu nutzen, um die Formulierungen der Verordnung mit allen Betroffenen zu diskutieren. In den letzten Jahren konnten wir wertvolle Daten sammeln und die darauf basierenden Analysen teilen wir selbstverständlich gerne. Die Erfahrung aus dem letzten Arbeitskreis hat gezeigt, dass eine produktive Zusammenarbeit zwischen allen Beteiligten möglich ist und zu guten Ergebnissen führt.

5. Teilautomatisiertes Verfahren (§ 16)

Wir sehen die Zulassung von teil- und vollautomatisierten Verfahren in §§ 16 und 17 als eine positive Ergänzung zu den aktuellen BaFin 3/2017 Vorgaben. Dadurch können VideoIdent-Verfahren schneller, benutzerfreundlicher und kostengünstiger abgewickelt werden. Im Hinblick auf die Wettbewerbsfähigkeit aller Dienstleister, die den Anforderungen des Geldwäschegesetzes und des BaFin Rundschreibens 3/2017 unterliegen, ist dies sehr zu begrüßen.

Die Vorgaben in Abschnitt § 16 wurden innerhalb der Branche weitgehend positiv, aber auch unterschiedlich aufgefasst. Wir ersuchen Sie daher, durch präzisere Formulierungen beide Absätze zu stärken, um gleiche Wettbewerbsbedingungen zu schaffen.

Im Mittelpunkt der Identitätslösungen stehen Sicherheit, Vertrauen und die Fähigkeit, eine Plattform mit benutzerfreundlichen Optionen anzubieten. Aufgrund unserer Erfahrung glauben wir, dass eine Kombination aus hochentwickelter Technologie mit KI-Algorithmen und menschlicher Interaktion, unter der Leitung von speziell geschultem Personal, eine der besten Möglichkeiten bietet, verschiedene Arten von Betrug zu erkennen.

Die hybride Interaktion zwischen Mensch und Maschine ist essenziell: Ein geschulter Mitarbeiter kann während eines Videoanrufs gezielte Fragen stellen und das Verhalten der zu identifizierenden Person beobachten (zittern die Hände? wirkt sie gestresst? scheint sie unter Druck zu agieren?) und am Ende des Videocalls bzw. am Ende einer vollautomatisierten Lösung eine manuelle Überprüfung durchführen, um die endgültigen Ergebnisse zu kontrollieren. Dies trägt wesentlich zur Vermeidung von Betrugsfällen in unserer Produktplattform bei.

Unsere Erfahrung zeigt ganz klar: Nicht die Frage, ob Mensch oder Maschine die besten Möglichkeiten bietet, ist entscheidend, sondern die Nutzung von Mensch und Maschine mit ihren jeweiligen Stärken.

Im Folgenden möchten wir anhand von zwei Beispielen aufzeigen, wie IDnow Betrug bekämpft und welche Maßnahmen wir dafür als wesentlich erachten.

Angriffe auf Identifizierungverfahren

Es gibt verschiedene Arten von Betrug, darunter Betrug an den biometrischen Daten eines Benutzers und physische oder digitale Angriffe auf das Ausweisdokument.

IDnow deckt verschiedene Arten von Betrug auf:

- Social Fraud, wie Social Engineering und Finanzagenten, ist weiterhin das größte Betrugsrisiko, bei IDnow machen sie 76% aller verzeichneten Angriffe aus.
- Angriffe mit gefälschten Ausweisen: 9% aller verzeichneten Angriffe
- Ähnlichkeitsbetrug mit gestohlenen Ausweisen einer Person: 15% aller verzeichneten Angriffe
- Im Vergleich zu VideoIdent ist Social Fraud nur sehr schwer durch automatisierte Verfahren erkennbar
- Erste Angriffsversuche mit Deepfakes beobachtet[2]

Die Technologieanbieter sind sich solcher Angriffe bewusst. Erfolgreiche Anbieter haben sowohl interaktive als auch automatisierte Lösungen für Identitätsverfahren eingeführt. Bei IDnow kombinieren wir interaktive Komponenten mit geschulten Mitarbeitern und vollautomatisierte Elemente im VideoIdent-Prozess. Diese hybride Lösung stellt derzeit das effektivste Mittel zur Erkennung und zum Verständnis bestehender und neuer Betrugsarten dar.

Der Identifizierungsprozess gilt nur dann als erfolgreich, wenn sowohl der Mitarbeiter als auch die Maschine ihr „OK“ geben. Es ist wichtig zu betonen, dass der Mitarbeiter das Ergebnis der Maschine im Identifizierungsprozess nicht sieht, um sicherzustellen, dass sich der Mensch nicht nur auf die Maschine verlässt.

Ein hybrides Modell, das KI und menschliche Intelligenz kombiniert, bietet den bestmöglichen Schutz für die Daten der Kunden und gewährleistet höchste Sicherheit. Durch Echtzeitfragen und trainierte Beobachtungen können unsere Mitarbeiter zusammen mit KI-Systemen effektiv arbeiten. Auch sogenannte Deepfakes, täuschend echt aussehende manipulierte Bild-, Audio- oder Videoaufnahmen, lassen sich durch das Zusammenspiel von Mensch und Maschine weitaus zuverlässiger erkennen als durch automatisierte Prozesse allein.

Angriff durch den Chaos Computer Club (CCC)

Die vom Chaos Computer Club (CCC) im Jahr 2022 gezeigten Angriffe auf Identitätsverfahren sind ein gutes Beispiel für die Vorteile eines hybriden Identitätsnachweisverfahrens. Bei dem CCC-Angriff wurden Computergrafiken verwendet, um die Informationen auf dem Ausweis digital zu verändern. Dennoch konnten sowohl Mitarbeiter als auch die automatischen Komponenten von IDnow diesen

[2] IDnow Trend Report: Fraud https://www.idnow.io/portfolio/idnow-trend-report/

Angriff, der auf unser VideoIdent-Produkt abzielte, erkennen und die Identifizierung als Betrug markieren. Anbieter von vollautomatisierten Verfahren konnten diese Angriffe jedoch nicht erkennen und wurden überlistet.

Dieses Beispiel zeigt eindrucksvoll, wie wichtig die interaktive Komponente zwischen Nutzer und Mitarbeiter in Form eines Video-Chats ist, die einen überaus wertvollen Beitrag zur Betrugsbekämpfung leistet.

Obwohl KI-Algorithmen inzwischen als zentrale Ergänzung zur menschlichen Überprüfung angesehen werden, können sie die interaktive Komponente derzeit nicht ersetzen. Algorithmen sind nicht in der Lage, neue Betrugsfälle allein zu verstehen und zu erkennen. Geschulte Mitarbeiter sind unerlässlich, um ungewöhnliche Verhaltensweisen zu identifizieren und richtig einzuordnen, wodurch die Sicherheit des Identifizierungsprozesses erheblich gesteigert wird.

Social Engineering

Betrüger manipulieren ahnungslose Personen, sich mit ihrem gültigen Ausweis für einen Dienst zu registrieren. Anschließend übernehmen sie das Konto, um durch Abhebungen oder Online-Überweisungen Geld zu erbeuten. Diese Form des Social Engineering ähnelt dem "Enkeltrick", ist jedoch auf die digitale Welt zugeschnitten.

Opfer werden häufig direkt von Betrügern über Plattformen wie Facebook Messenger oder WhatsApp kontaktiert oder klicken auf täuschend echte Anzeigen oder Werbeangebote im Internet. Den Opfern wird eine glaubhafte Geschichte präsentiert, die sie dazu verleitet, ein Konto zu eröffnen. Sozialer Betrug, wie Social Engineering und Finanzagenten, stellt weiterhin das größte Betrugsrisiko dar und macht bei IDnow 75 % der Betrugsfälle aus.[3]

Diese Form von Angriff lässt sich nur in einem Video-Chat erkennen. Bei vollautomatisierten Verfahren gibt es keine Ansatzpunkte, um solche Angriffe zu identifizieren. Unsere Identifizierungsexperten stellen in einem leicht verständlichen, agentengestützten Videoanruf sicher, dass der Benutzer wirklich derjenige ist, für den er sich ausgibt.

Um zu gewährleisten, dass ein Kunde nicht unter Zwang oder Manipulation handelt, sind unsere Experten darin geschult, sein Verhalten zu beobachten. Sie achten beispielsweise auf:

[3] IDnow Sicherheitsbericht 2020

- Der Zweck der Identifizierung wird abgefragt (identifiziert sich der jeweilige Endnutzer für sich oder andere, für welchen Anbieter und aus welchem Grund). Hier wird bei Bedarf oder bei vorliegender Inkonsistenz der Antworten nachgehakt.
- Auch die Möglichkeit weitere Fragen einzubauen, wird von vielen Banken wahrgenommen: z. B., ob man eine Einladung per E-Mail erhalten hat, ob man von Dritten angesprochen wurde, etc. Dies wäre ein Indikator, dass die zu identifizierende Person auf einen Betrug reingefallen ist. Das Verfahren kann dementsprechend abgebrochen werden und die zu identifizierende Person vor enormen finanziellen Schaden bewahrt werden.
- Zudem setzen die geschulten Mitarbeiter von IDnow während des Identifizierungsprozesses gezielt Techniken ein. Beispielsweise werden zu bestimmten Zeitpunkten persönliche Daten abgefragt, die der Anwender auswendig kennen müsste, wie Geburtsort oder Geburtsdatum. Kann der Anwender diese Daten nicht sofort beantworten und muss nachsehen, deutet dies auf möglichen Betrug hin.
- Weitere von IDnow verwendete Betrugsindikatoren zielen auf das Beobachten der zu identifizierenden Person ab – zittern ihre Hände, ist sie nervös, scheint sie unter Druck zu agieren?

Das Ziel von IDnow ist es nicht nur, Betrugsversuche zu stoppen, sondern auch sicherzustellen, dass sie sich nicht wiederholen. Unser Qualitätsmanagement arbeitet eng mit der örtlichen Polizei zusammen, um kriminelle Organisationen zu stoppen und sicherzustellen, dass gefälschte Websites aus dem Internet entfernt werden.

Formulierungsvorschläge

Bitte erwägen Sie, deutlicher zu formulieren, was genau mit Teilautomatisierung gemeint ist.

Formulierungsvorschlag

§ 16: Soweit die übrigen Voraussetzungen dieses Abschnitts**, insbesondere bezüglich der audiovisuellen Kommunikation zwischen dem Mitarbeiter und der zu identifizierenden Person, vorliegen**, können teilautomatisierte Verfahren zur Identifizierung Anwendung finden, wenn (…)

Bei der Teilautomatisierung ist unklar was genau „Echtzeit“ und „ohne Unterbrechung“ bedeuten soll. Es sollte klargestellt werden dass hiermit zum einen gemeint ist dass der Prozess nicht untergebrochen

und später wiederaufgenommen werden darf und dass die audiovisuelle Kommunikation in Echtzeit erfolgen muss.

Formulierungsvorschlag

§ 9 (2): Die Durchführung der Videoidentifizierung, **der Teilautomatisierung oder der Vollautomatisierung darf nicht unterbrochen werden. Wird unterbrochen, so ist der Prozess wieder von Anfang an durchzuführen.**

Die audiovisuelle Kommunikation hat in Echtzeit zu erfolgen.

IDnow empfiehlt zudem, dass die Gegenmaßnahmen gegen Social Engineering im interaktiven Teil stattfinden müssen, da diese nur von einem Menschen sinnvoll erkannt werden können.

Formulierungsvorschlag

§ 16 (1): lediglich die Aufzeichnung nach § 9 Absatz 5 und die nach §§ 11 und **12 (1) und 12 (4)** vorgeschriebenen Prüfungen und die hierfür notwendige Kommunikation mit der zu identifizierenden Person automatisiert erfolgt und

IDnow empfiehlt zudem Klarstellung hinsichtlich des Endes des VideoIdent-Prozesses. Die Anforderung, die Aufzeichnungs- und Ergebnisdatei mit der Bank zu teilen, ist unklar. Im Entwurf heißt es, dass dies geschehen muss, bevor der Videoprozess abgeschlossen ist. Wenn man jedoch davon ausgeht, dass der Prozess abgeschlossen ist, wenn der Agent die SMS-TAN sendet, dann bleibt nicht genug Zeit, um die Ergebnisdatei zu überprüfen. Der Benutzer würden in diesem Fall unnötig warten müssen. Die Aufzeichnung und die Ergebnisdatei sollten nach dem VideoIdent-Vorgang überprüft und an die Bank gesendet werden.

Formulierungsvorschlag

§ 16 (2): diese Aufzeichnung und das Ergebnis der Überprüfung vor **Übermittelung** des Identifizierungsvorgangs **an den Verpflichteten** von einem Mitarbeiter detailliert auf Einhaltung der Vorgaben nach §§ 9, 11 und 12 geprüft werden.

6. Vollautomatisiertes Verfahren (§ 17)

Das vollautomatisierte Verfahren stellt eine spannende Innovation im Bereich der digitalen Identifikationslösungen dar. Es ist jedoch essenziell, dass dabei ein Mindeststandard an Sicherheit gewährleistet bleibt. Der derzeitige Wortlaut von § 17 lässt jedoch viele Fragen offen und schafft Unsicherheit in der Branche.

Das Fehlen klarer Definitionen und Kriterien kann dazu führen, dass möglichst kostengünstige Verfahren angeboten werden, die möglicherweise keine ausreichend sicheren Standards erfüllen („Race to the Bottom“). Diese Situation zu vermeiden, liegt sicherlich in unser aller Interesse und sollte daher durch unmissverständliche Formulierungen geklärt werden.

- Wir bitten um eine genauere Spezifizierung, insbesondere welche Verfahren als "gleichwertig" anzusehen sind und wie die Definition für "gleichwertig" lautet.
- Bitte erläutern und definieren Sie eine Reihe von Kriterien, die zur Bestimmung gleichwertiger Prozesse verwendet werden können.
- Auch die Anforderungen an die Prüfung und die anschließenden Versuche sollten ausführlicher beschrieben werden.
- Ein Zertifizierungsverfahren sollte in Betracht gezogen werden, um die Erfüllung von Mindestanforderungen zu gewährleisten.

Des Weiteren scheint die aktuelle Formulierung die Möglichkeit offenzulassen, die Anforderungen aus allen vorherigen Paragrafen zu ignorieren was vermutlich nicht beabsichtigt ist.

Formulierungsvorschlag

§ 17 (1): Bei einem Verfahren, das einen über § 16 hinausgehenden Automatisierungsgrad aufweist, kann eine Eignung zur geldwäscherechtlichen Überprüfung der Identität erprobt werden **soweit die übrigen Voraussetzungen dieses Abschnitts eingehalten werden**.

7. Identifizierung mit NFC / BAC

Eine weitere Möglichkeit, die aktuell nicht in der Verordnung enthalten ist, wäre die Nutzung von NFC für Dokumente wie Reisepässe. Mittels „Basic Access Control“ (BAC) könnten dabei Daten wie Name, Geburtsdatum, Passnummer, Staatsangehörigkeit, Geschlecht, Gültigkeitsdauer des Passes und das Lichtbild ausgelesen werden. Das Lichtbild könnte dann für einen biometrischen Vergleich verwendet werden. Wenn diese Methode, wie in § 16 beschrieben, mit einer interaktiven Kommunikation zwischen Mitarbeiter und Nutzer kombiniert wird, könnte dies ein sicheres und nutzerfreundliches Verfahren darstellen.

Derzeit ist diese Form der Identifizierung nach unserem Verständnis jedoch nicht möglich, da das Passgesetz in § 16 ff explizit vorschreibt, dass nur Behörden den Chip auslesen dürfen und nichtöffentlichen Stellen das Auslesen biometrischer Daten untersagt ist. Hier müsste eine Anpassung des Gesetzes erfolgen, um diese Form der Identifizierung zu ermöglichen. Wir regen daher an, zu prüfen, ob eine solche Gesetzesänderung möglich ist.

Ähnliche Einschränkungen finden sich auch in den Gesetzen anderer Länder. So untersagt beispielsweise auch Frankreich explizit das Auslesen von Pässen durch nichtstaatliche Stellen

8. Fazit

Die Digitalisierung ist seit vielen Jahren ein Thema auf jeder politischen Agenda. Nach jeder Legislaturperiode bleibt festzustellen, dass der Erlass von Gesetzen oder Verordnungen allein nicht zum Ziel führt, auch die praktische Umsetzbarkeit muss im Fokus der Regulierung stehen und berücksichtigt werden.

Wir sind der Meinung, dass Sicherheit nicht nur ordnungspolitisch gedacht werden darf, sondern auch die praktische Umsetzung und bürgernahe Prozesse im Vordergrund stehen müssen, um ein **möglichst hohes Maß an praktikabler** Sicherheit zu erreichen.

Wir glauben, dass die Wiederbelebung des BMF-Arbeitskreises Fernidentifizierung im Rahmen dieses Referentenentwurfs ein hervorragender Ausgangspunkt für weitere Diskussionen wäre, um die Zusammenarbeit zwischen den Akteuren des öffentlichen und privaten Sektors in dieser Übergangszeit bis zum Inkrafttreten der EU-GwG-Verordnung und der EU Digital Identity Wallets zu fördern.

Wir sprechen uns klar für die Beibehaltung der im BaFin-Rundschreiben 3/2017 festgelegten Standards und Anforderungen für Ausweisdokumente aus. Diese Kriterien haben sich bewährt und zu sicheren Onboarding-Prozessen geführt. Der aktuelle Entwurf wird nicht das gewünschte Ergebnis erzielen – die wirksame Betrugsbekämpfung und die Bereitstellung von Lösungen für deutsche und ausländische Ausweisinhaber, die eine Identitätsprüfung für digitale Dienstleistungen benötigen.

Für den Inhalt ist die Geschäftsführung verantwortlich

IDnow GmbH
Auenstraße 100
80469 München
+49 89 413 24 600
www.idnow.io

Annex I: Spezifische Textvorschläge

GWVideoIdentV Originaltext	IDnow Textvorschläge	IDnow Begründung
§ 1 Regelungsbereich (1) Diese Verordnung regelt die Zulassung des Videoidentifizierungsverfahrens nach § 13 Absatz 2 Nummer 2 des Geldwäschegesetzes. (2) Die Anforderungen an die angemessene Prüfung eines vor Ort vorgelegten Dokuments nach § 13 Absatz 1 Nummer 1 des Geldwäschegesetzes werden durch diese Verordnung nicht berührt.		
§ 2 Begriffsbestimmungen (1) Videoidentifizierungsverfahren im Sinne dieser Rechtsverordnung sind Verfahren zur Identifizierung von natürlichen Personen, bei denen ungeachtet der räumlichen Trennung eine sinnliche Wahrnehmung der am Identifizierungsprozess beteiligten Personen und deren Ausweisdokumente mittels des Einsatzes von bildgebenden Kommunikationstechnologien möglich ist. (2) Teilautomatisierte Videoidentifizierungsverfahren im Sinne dieser Rechtsverordnung sind Verfahren, bei denen einzelne Schritte der Identifizierung und Prüfung durch ein IT-System durchgeführt werden. (3) Mitarbeiter im Sinne dieser Rechtsverordnung sind Personen, die beim Verpflichteten nach § 2 Absatz 1 des Geldwäschegesetzes oder beim Dritten, auf den der Verpflichtete zur Identifizierung nach § 17 Absatz 1 und 5 des Geldwäschegesetzes zurückgreift, Aufgaben		

wahrnehmen, um die Identifikation nach den in dieser Verordnung beschriebenen Verfahren durchzuführen.		
§ 3 Verantwortlichkeit der Verpflichteten Die Verantwortung für die Durchführung der Identifizierung einschließlich der Erfüllung der Anforderungen der folgenden Abschnitte an die Verfahren liegt bei den Verpflichteten nach § 2 Absatz 1 des Geldwäschegesetzes, auch soweit sie sich zur Durchführung der Sorgfaltspflichten eines Dritten bedienen.		
Abschnitt 2 Videoidentifizierungsverfahren		
§ 4 Eignung zur geldwäscherechtlichen Identifizierung Die Identifizierung durch ein Videoidentifizierungsverfahren oder teilautomatisiertes Videoidentifizierungsverfahren ist zur Erfüllung der Pflichten nach §§ 11 bis 13 des Geldwäschegesetzes geeignet, wenn die Voraussetzungen dieses Abschnitts erfüllt sind.	Die Identifizierung durch ein Videoidentifizierungsverfahren oder teilautomatisiertes oder **vollautomatisiertes** Videoidentifizierungsverfahren ist zur Erfüllung der Pflichten nach §§ 11 bis 13 des Geldwäschegesetzes geeignet, wenn die Voraussetzungen dieses Abschnitts erfüllt sind.	Lediglich das teilautomatisierte Videoidentifikationsverfahren wird erwähnt. Wie steht es um vollautomatisierte Verfahren?
§ 5 Anwendungsbereich (1) Das Videoidentifizierungsverfahren und das teilautomatisierte Videoidentifizierungsverfahren können für Identifizierungen durch alle Verpflichtete nach § 2 Absatz 1 des GwG verwendet werden, soweit die zuständigen Aufsichtsbehörden nach § 50 des Geldwäschegesetzes dies in ihren Auslegungs- und Anwendungshinweisen nach § 51 Absatz 8 des Geldwäschegesetzes nicht ausschließen. (2) Das Videoidentifizierungsverfahren und das teilautomatisierte Videoidentifizierungsverfahren dürfen nur verwendet werden, wenn	§ 5(2): Das Videoidentifizierungsverfahren und das teilautomatisierte **sowie das vollautomatisierte** Videoidentifizierungs-verfahren dürfen nur verwendet werden, wenn der Verpflichtete für diesen Identifizierungsvorgang **mindestens** in gleichwertiger Art und Weise auch ein Verfahren zur Überprüfung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anbietet **sofern die**	Das vollautomatisierte Verfahren wird auch hier nicht erwähnt. Außerdem empfiehlt IDnow, "mindestens in gleichwertiger Art und Weise " einzufügen, wenn betont werden soll, dass die eID als erstes Identifikationsverfahren angeboten werden soll. Die Beibehaltung des Verfahrens durch Videoidentifizierung ist

der Verpflichtete für diesen Identifizierungsvorgang in gleichwertiger Art und Weise auch ein Verfahren zur Überprüfung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anbietet.	**Nutzung des elektronischen Identitätsnachweises durch den Nutzer bei diesem Vorgang möglich ist**.	essenziell um nicht-deutsche Staatsbürger sowie nicht-ortsansässige Entitäten identifizieren zu können. Dies wird auch in Sektion A Problem und Ziele des GWVideoIdentV neben dem Kostenfaktor als eines der Hauptziele genannt.
§ 6 Identifizierung durch geschulte Mitarbeiter (1) Eine Videoidentifizierung darf nur von entsprechend geschulten und hierfür ausgebildeten Mitarbeitern des Verpflichteten oder eines Dritten, auf den der Verpflichtete zur Identifizierung nach § 17 Absatz 1 und 5 des Geldwäschegesetzes zurückgreift, durchgeführt werden. Eine weitere Auslagerung auf einen weiteren Dritten ist nicht zulässig. (2) Die Mitarbeiter müssen über einen aktuellen Kenntnisstand verfügen bezüglich 1. der mittels Videoidentifizierung prüfbaren Merkmale derjenigen Dokumente, die im Rahmen des Videoidentifizierungsverfahrens akzeptiert werden, 2. der anzuwendenden Prüfverfahren, 3. der aktuellen Fälschungsmöglichkeiten dieser Dokumente, 4. der maßgeblichen geldwäscherechtlichen und datenschutzrechtlichen Vorschriften und 5. der Regelungen in diesem Abschnitt. Zu den akzeptierten Dokumenten, ihren prüfbaren Merkmalen, der anhand dieser Merkmale durchzuführenden Prüfung und den entsprechenden Schulungsmaßnahmen muss den Mitarbeitern eine geeignete Dokumentation vorliegen.	Eine weitere Auslagerung auf einen weiteren Dritten ist **nur dann zulässig, wenn durch vertragliche Vereinbarung entsprechender Verpflichtungen zugunsten der Verpflichteten, der weitere Dritte zur Einhaltung der (gesetzlichen) Vorgaben für die Erfüllung der Sorgfaltspflichten und zur Einräumung von Prüf- und Kontrollrechten für den Verpflichteten und dessen Aufsichtsbehörde verpflichtet wird**.	IDnow bittet um Klarstellung hinsichtlich der erlaubten Outsourcing-Möglichkeiten, insbesondere im Hinblick auf externe Callcenter (1) zur Identifizierung. Verbot der Sub-Auslagerung wurde nach BaFin 2017 durch vertragliche Vereinbarungen zwischen dem weiteren Dritten und dem Verantwortlichen geheilt. Dies sollte zur Vermeidung von Verwirrung klargestellt werden.

(3) Die vorgenannten Inhalte müssen den Mitarbeitern vor Aufnahme ihrer Identifizierungstätigkeit angemessen vermittelt und nachfolgend in regelmäßigen Abständen, mindestens einmal jährlich, sowie bei Bedarf aktualisiert werden. Ein Bedarf kann in einer Änderung der gesetzlichen Anforderungen, der Einführung eines neuen Dokumentenmodells oder eines neuen Sicherheitsmerkmals, im Falle eines Auftretens einer signifikanten Zahl von Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstigen Fehlern im Verfahrensablauf begründet sein. (4) Die Mitarbeiter müssen in regelmäßigen Abständen an Aus- und Fortbildungen zum Thema digitaler Sicherheit mit besonderem Fokus auf das Erkennen von Täuschungen und technischen Angriffen teilnehmen. Diese Schulungen sind mindestens einmal im Jahr durchzuführen.		
§ 7 Räumlichkeiten Die Mitarbeiter müssen sich während der Identifizierung in abgetrennten und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.	Anwendbare technische Norm(en): ETSI EN 319 401 ETSI TS 119 461 ISO 27001 BSI TRs	IDnow bittet um Klärung des Begriffs "Zugangskontrolle" und empfiehlt, zur weiteren Spezifizierung der Anforderungen auf technische Normen zu verweisen. Generell sind die Anforderung sehr gering und würden noch nicht mal den Anforderungen der GDPR entsprechen.
§ 8 Einverständnis (1) Eine Identifizierung darf nur dann erfolgen, wenn die zu identifizierende Person zu Beginn des	(1) Eine Identifizierung darf nur dann erfolgen, wenn die zu identifizierende Person zu Beginn des Videoidentifizierungsverfahrens ihr	Wie soll die Zustimmung erfolgen? Durch simples Ankreuzen eines Kontrollkästchens oder innerhalb des Videocalls? IDnow empfiehlt

Videoidentifizierungsverfahrens ihr ausdrückliches Einverständnis damit erklärt hat, dass der gesamte Identifizierungsprozess aufgezeichnet und Bildaufnahmen ihrer Person und ihres Ausweisdokuments angefertigt werden. (2) Die Erklärung des Einverständnisses ist aufzuzeichnen und aufzubewahren. § 8 des Geldwäschegesetzes gilt entsprechend.	ausdrückliches Einverständnis damit erklärt hat, dass der gesamte Identifizierungsprozess aufgezeichnet und Bildaufnahmen ihrer Person und ihres Ausweisdokuments angefertigt werden. **Das Einverständnis verbal innerhalb des Gesprächs oder durch eine technische Lösung erfolgen.**	einen Kontrollkästchens, da dies der Standard ist und eine verbale Zustimmung keinerlei Vorteile bietet.
§ 9 Technische und organisatorische Anforderungen (1) Bei der Zuteilung der Identifizierungsvorgänge an die Mitarbeiter müssen Mechanismen eingesetzt werden, die einer vorhersehbaren Zuteilung von Fällen und damit der dadurch bestehenden Möglichkeit einer Manipulation entgegenwirken. (2) Die Durchführung der Videoidentifizierung muss in Echtzeit und ohne Unterbrechung erfolgen. (3) Die audiovisuelle Kommunikation zwischen dem Mitarbeiter und der zu identifizierenden Person ist in Bezug auf Integrität und Vertraulichkeit ausreichend abzusichern. Aus diesem Grund sind nur Ende-zu-Ende verschlüsselte Videoübertragungen zulässig. Es sind hierbei die Empfehlungen der Technischen Richtlinie TR-03116 des Bundesamtes für Sicherheit in der Informationstechnik einzuhalten. (4) Die Bild- und Tonqualität der Kommunikation muss in einem ausreichenden Maße gegeben sein, um eine zweifelsfreie Identifizierung anhand aller geforderten Prüfungen uneingeschränkt zu ermöglichen. Hierzu zählen insbesondere die Prüfungen der als im Weißlicht visuell prüfbar eingestuften Sicherheitsmerkmale sowie die Prüfung auf Beschädigung und Manipulation des Dokuments. Hierfür darf die Auflösung der übertragenen Bilddaten den Wert 720p: 1280 x 720 bei 25 Frames pro Sekunde zu keinem Zeitpunkt	§ 9 (2): Die Durchführung der Videoidentifizierung, **der Teilautomatisierung oder der Vollautomatisierung darf nicht unterbrochen werden. Wird unterbrochen, so ist der Prozess wieder von Anfang an durchzuführen.** **Die audiovisuelle Kommunikation hat in Echtzeit zu erfolgen.** (3) […] Es sind hierbei die Empfehlungen der Technischen Richtlinie **TR-02102** des Bundesamtes für Sicherheit in der Informationstechnik einzuhalten. **(6) Es sind die relevanten Anforderung der Durchführungsverordnung (EU) 2015/1502 einzuhalten.**	IDnow bittet um Klarstellung der Definition von "Echtzeit und ohne Unterbrechung für teilautomatisierte Prozesse" iRv teilautomatisierten Verfahren §9(2). Ist es beabsichtigt, dass hier TR-03116 zu Anwendung kommt? Diese gilt typischerweise für Projekte der Bundesregierung. Eventuell ist die TR-02102 besser geeignet. Ein Verweis auf die Anforderung der eIDAS könnte die GWVideoIdentV besser in Einklang bringen mit den Anforderungen die aus §22 der AMLR kommen werden.

unterschreiten. Die übertragene Bildqualität muss der von dieser Auflösung zu erwartenden Qualität entsprechen. (5) Im Rahmen der Videoübertragung sind durch den jeweiligen Mitarbeiter Bildaufnahmen anzufertigen, auf denen die zu identifizierende Person sowie Vorder- und Rückseite des von dieser zur Identifizierung verwendeten Ausweisdokuments und die darauf jeweils enthaltenen Angaben zweifelsfrei erkennbar sind.		
§ 10 Geeignete Ausweisdokumente (1) Die Ausweisdokumente, anhand derer die Identität der zu identifizierenden Person festgestellt werden soll, müssen die in den Absätzen 2 bis 4 genannten Anforderungen erfüllen. (2) Das Ausweisdokument muss mindestens jeweils ein prüfbares Sicherheitsmerkmal aus den in § 11 Absatz 4 aufgeführten Kategorien enthalten. (2) Beinhaltet ein Ausweisdokument als einziges prüfbares Merkmal in der Kategorie des § 11 Absatz 4 Nummer 1 das Merkmal des Buchstaben e, ist das Ausweisdokument abweichend von Satz 1 nur dann zuzulassen, wenn aus den anderen beiden Kategorien des genannten Absatzes insgesamt drei prüfbare Merkmale vorhanden sind. (2) Als prüfbar gilt ein Sicherheitsmerkmal dann, wenn für das Sicherheitsmerkmal geeignetes Referenzmaterial vorliegt. Als geeignet gilt das Referenzmaterial für ein bestimmtes Merkmal, wenn		Die Anforderungen sollten wieder in Einklang mit dem Rundschreiben 3 / 2017 gebracht werden. Alternativ schlagen wir die Nutzung des Arbeitskreises Fernidentifizierung vor um die Änderungen zu diskutieren.

1. Motiv, Position und relative Größe des Merkmals auf dem Dokument sowie für Merkmale in der Kategorie des § 11 Absatz 4 Nummer 1 der Verlauf von Veränderungen des Merkmals bei unterschiedlichem Betrachtungswinkel aus dem Referenzmaterial hervorgehen, 2. der für das jeweilige Merkmal erforderliche Detailgrad des Referenzmaterials im Abbildungs- oder Videoformat einen sachgerechten Abgleich ermöglicht. (3) Das Ausweisdokument enthält mindestens eine beugungsoptisch wirksame Struktur im Lichtbildbereich. (3) Darüber hinaus enthält das Dokument mindestens eine Prägung im Bereich individueller Eintragungen oder mindestens eine taktile individuelle Eintragung. (4) Das Ausweisdokument enthält mindestens ein Sekundärlichtbild und einen maschinenlesbaren Bereich. (5) Für gültige Reisepässe der Vereinigten Staaten von Amerika ohne Vollkunststoff-Personaldatenseiten wird unwiderlegbar vermutet, dass sie die in den Absätzen 2 bis 4 genannten Voraussetzungen erfüllen.		

§ 11 Überprüfung des Ausweisdokuments (1) Um sich über die Identität der zu identifizierenden Person mittels eines nach § 10 zulässigen Ausweisdokumentes zu vergewissern, hat der Mitarbeiter das jeweilige Ausweisdokument wie folgt zu prüfen: 1. Überprüfung auf Verfälschungen oder Manipulationen nach Absatz 2, 2. Überprüfung der Gültigkeit und Plausibilität nach Absatz 3, 3. Überprüfung auf optische Sicherheitsmerkmale nach Absatz 4, 4. Überprüfung auf Richtigkeit sekundärer Merkmale nach Absatz 5. (2) Das Ausweisdokument ist darauf zu überprüfen, ob es unbeschädigt und nicht manipuliert ist. Dies beinhaltet die Prüfung der Merkmale und Daten nach § 10 Absatz 3 und 4. Vorhandene Sekundärlichtbilder sind zu prüfen und mit den übrigen Lichtbildern abzugleichen. Darüber hinaus beinhaltet dies die Prüfung der Dokumentenoberfläche, insbesondere im Lichtbildbereich, und aller weiteren in Sicherheitsmerkmalen integrierten Individualdaten, die mit den in der visuellen Zone integrierten Daten abzugleichen sind; dabei sind alle Sicherheitsmerkmale, in denen Individualdaten enthalten sind, auf Echtheit zu prüfen. (3) Der Mitarbeiter hat eine Gültigkeits- und Plausibilitätsprüfung der auf dem Ausweis enthaltenen Daten und Angaben vorzunehmen. Dies beinhaltet insbesondere die Überprüfung, ob Ausstellungsdatum und Gültigkeitsdatum des Ausweisdokumentes zueinander passen. Das Ausstellungsdatum darf insbesondere nicht in der Zukunft liegen. Ferner darf die Gültigkeitsdauer des vorgelegten Ausweisdokumentes nicht gegen die für Ausweisdokumente dieser Art geltende Norm verstoßen.		Die Anforderungen sollten wieder in Einklang mit dem Rundschreiben 3 / 2017 gebracht werden. Alternativ schlagen wir die Nutzung des Arbeitskreises Fernidentifizierung vor um die Änderungen zu diskutieren.

Zwingender Bestandteil der Überprüfung ist zudem eine automatisierte Berechnung der in der maschinenlesbaren Zone enthaltenen Prüfziffern sowie ein Kreuzvergleich der in ihr enthaltenen Angaben mit den Angaben im Sichtfeld des Ausweisdokumentes. Außerdem sind die Schreibweise der Ziffern, die Behördenkennziffer und die verwendeten Schriftarten auf Auffälligkeiten zu überprüfen. (4) Das Ausweisdokument ist darauf zu überprüfen, ob im Weißlicht visuell zu erkennende optische Sicherheitsmerkmale im Hinblick auf Form und Inhalt zu den auf dem Ausweisdokument enthaltenen individuellen Merkmalen passen und mit Referenzmaterial aus einer Ausweisdatenbank übereinstimmen. Zu den optischen Sicherheitsmerkmalen zählen insbesondere: 1. Kategorie beugungsoptisch wirksame Merkmale: a) Identigram, b) Zero-Order-Device, c) 3D-Relief-Effekt, d) achromatische Strukturen, e) chromatische, kinematische Strukturen, 2. Kategorie Personalisierungstechnik: a) Laserkippbild, b) taktile Bereiche, c) Laserperforation mit Individualdaten des Dokumentinhabers, 3. Kategorie Material: a) Prägung, b) transparentes Fenster. Die Prüfung der optischen Merkmale gilt als erfolgreich, wenn jeweils ein zufällig ausgewähltes Merkmal aus den in Satz 2 aufgeführten einzelnen Kategorien erfüllt wird.		

Ferner ist bei den Merkmalen aus der in Satz 2 unter Nummer 1 aufgeführten Kategorie zu beachten, dass die Merkmale a) und b) bevorzugt zu prüfen sind und Merkmal e) nur in dem Falle herangezogen werden darf, wenn keine anderen Merkmale aus dieser Kategorie vorhanden sind. Wird Merkmal e) geprüft, muss die Prüfung besonders detailliert erfolgen und es müssen mindestens drei Merkmale aus den anderen beiden Kategorien geprüft werden. Die Abfrage der Merkmale nach Satz 5 darf nicht nach einem festgelegten Rhythmus erfolgen. Abweichend von Satz 3 gilt die Prüfung der optischen Merkmale für Ausweisdokumente im Sinne von § 10 Absatz 5 als erfolgreich, sofern sowohl ein optisches Sicherheitsmerkmal nach Satz 2 Nummer 1 Buchstabe e) als auch ein Wasserzeichen erfüllt werden. (5) Das Ausweisdokument ist hinsichtlich der sonstigen enthaltenen, im Weißlicht visuell zu erkennenden und einer Kontrolle zugänglichen formalen Merkmale auf die Richtigkeit sekundärer Merkmale des Dokuments zu überprüfen, insbesondere auf Typographie, Farben, Schriftart, Zeichenabstand, Zeichengröße sowie Prüfziffern in der maschinenlesbaren Zone. (6) Für die Prüfschritte der Absätze 2 bis 5 ist jeweils zu dokumentieren, welche Merkmale geprüft wurden und welches Prüfergebnis für jedes geprüfte Merkmal festgestellt wurde.		
§ 12 Überprüfung der zu identifizierenden Person (1) Der Mitarbeiter muss sich davon überzeugen, dass das Lichtbild und die Personenbeschreibung auf dem verwendeten Ausweisdokument zu der zu identifizierenden Person passen. Lichtbild, Ausstellungsdatum und Geburtsdatum müssen ebenfalls zueinander kohärent sein.		IDnow empfiehlt, diesen Schritt (insbesondere (2) und (3)) auf Grund der Gefahr von Social Engineering nicht zu automatisieren, sondern ein interaktives Gespräch zwischen zu identifizierender Person und geschultem Mitarbeiter

(2) Der Mitarbeiter muss sich durch psychologische Fragestellungen und Beobachtungen während der Durchführung des Identifizierungsvorgangs von der Plausibilität der Angaben im Ausweisdokument, der Angaben der zu identifizierenden Person im Gespräch sowie der angegebenen Absicht der zu identifizierenden Person überzeugen. Dabei können insbesondere Fragen nach dem Alter der Person für eine Validierung im Hinblick auf das Ausweisbild sowie die Geburtsangaben im Ausweisdokument erfolgen. Der Anlass für die Identifikation ist durch die zu identifizierende Person ausdrücklich zu benennen. (3) Die Mitarbeiter sind dahingehend zu schulen, dass sie feststellen können, ob die zu identifizierende Person nach eigenem Willen handelt. 4) Der Mitarbeiter muss sich davon überzeugen, dass sämtliche auf dem Ausweisdokument enthaltenen Angaben der zu identifizierenden Person mit gegebenenfalls bereits beim Verpflichteten vorhandenen und dem Mitarbeiter verfügbaren Daten übereinstimmen.		beizubehalten, wie im BaFin-Rundschreiben 03/2017 vorgesehen. Grund: Fast 70 % der von IDnow aufgedeckten Betrugsfälle sind Social Engineering geschuldet. Geschulte Mitarbeiter sind besser ausgebildet, dies aufzudecken als die Künstliche Intelligenz (KI).
§ 13 Abbruch des Videoidentifizierungsvorgangs (1) Ist die vorstehend beschriebene visuelle Überprüfung nicht möglich, ist der Identifizierungsprozess abzubrechen. Dies gilt insbesondere bei 1. unzureichenden Lichtverhältnissen, 2. unzureichender Bildqualität, 3. unzureichender Bildübertragung, 4. unzureichender sprachlicher Kommunikation mit der zu identifizierenden Person oder 5. bei sonstigen vorliegenden Unstimmigkeiten oder Unsicherheiten.	~~Der innere Gesichtsbereich zwischen Kinn und Stirnkante sollte zudem während des Identifizierungsvorgangs mindestens 50 % der Bildhöhe ausmachen und Reaktionsverzögerungen im Gesprächsverlauf und zur Umsetzung von Aufforderungen unterhalb von einer Sekunde liegen.~~	Unklar wie die Größenangabe zu interpretieren ist. Muss diese einmalig vorliegen oder ständig? 1 Sekunde Verzögerung bei der Antwort sollte geklärt werden - handelt es sich um eine etwaige Netzwerkverzögerung oder etwas anderes? Die Antwort des Nutzers auf die Anfrage des Agenten kann theoretisch beliebig lange dauern und sollte nicht auf 1 Sekunde

Bildqualität und Bildübertragung sind in der Regel unzureichend, wenn die Auflösung der übertragenen Bilddaten den Wert 720p: 1280 x 720 (Querformat, bei Hochformat 720 x 1280) bei 25 Frames pro Sekunde unterschreitet. Der innere Gesichtsbereich zwischen Kinn und Stirnkante sollte zudem während des Identifizierungsvorgangs mindestens 50 % der Bildhöhe ausmachen und Reaktionsverzögerungen im Gesprächsverlauf und zur Umsetzung von Aufforderungen unterhalb von einer Sekunde liegen. (2) Bei Abbruch des Verfahrens aus in Absatz 1 genannten Gründen kann die Identifizierung mittels eines anderen nach dem Geldwäschegesetz zulässigen Verfahrens vorgenommen werden.		begrenzt werden, zumal dies viel zu kurz bemessen ist
§ 14 Maßnahmen zur Verhinderung technischer Angriffe (1) Der Mitarbeiter hat sich durch die Anwendung geeigneter Maßnahmen davon zu überzeugen, dass kein Verfahren zur Manipulation der Videoübertragung verwendet wird. Zu geeigneten Maßnahmen zählen insbesondere folgende Aufforderungen gegenüber der zu identifizierenden Person: 1. der Bewegung von Augen, Augenlidern und Mund, 2. der Änderung des Abstands der Person von der Kamera oder 3. der Änderung von Beleuchtungsbedingungen. (2) Ergänzend zu Maßnahmen nach Absatz 1 muss die zu identifizierende Person im Rahmen der visuellen Prüfung das verwendete Ausweisdokument vor der Kamera nach Anweisung des Mitarbeiters horizontal und vertikal kippen. Zudem ist sie aufzufordern, an geeigneter Stelle variabel, systemseitig zufällig bestimmt, bestimmte sicherheitsrelevante Teile des Ausweisdokumentes zu bedecken und eine Hand vor ihrem Gesicht zu bewegen. Mittels hierbei gefertigter ausschnittvergrößerter Standbilder ist vom Mitarbeiter zu prüfen, ob die jeweiligen		Wir begrüßen die Beibehaltung dieses Schrittes als interaktives Gespräch zwischen zu identifizierende Person und geschultem Mitarbeiter. Durch ein persönliches Gespräch wird das Risiko von Video-Manipulation und Deepfakes wesentlich reduziert.

Sicherheitsmerkmale an entsprechender Stelle vollständig überdeckt werden und die Übergänge keinerlei Artefakte erkennen lassen, die auf eine Manipulation hindeuten.		
§ 15 Übermittlung einer Ziffernfolge; Abschluss des Verfahrens (1) Während der Videoübertragung übermittelt der Mitarbeiter eine eigens für diesen Zweck generierte und gültige Ziffernfolge an die zu identifizierende Person. Die Übermittlung kann insbesondere per E-Mail oder per SMS erfolgen. Die zu identifizierende Person hat diese im unmittelbaren Anschluss daran an den Mitarbeiter elektronisch zurückzusenden. (2) Das Verfahren ist abgeschlossen, wenn ein erfolgreicher Abgleich der Ziffernfolge nach Eingabe durch die zu identifizierende Person erfolgt ist.	(2) Das Verfahren ist **für die zu identifizierende Person** abgeschlossen, wenn ein erfolgreicher Abgleich der Ziffernfolge nach Eingabe durch die zu identifizierende Person erfolgt ist.	Es sollte eventuell klargestellt werden dass das Verfahren für den Nutzer abgeschlossen ist aber eventuell noch eine manuelle Überprüfung bei der Teilautomatisierung erfolgen muss.
§ 16 Einsatz teilautomatisierter Verfahren Soweit die übrigen Voraussetzungen dieses Abschnitts vorliegen, können teilautomatisierte Verfahren zur Identifizierung Anwendung finden, wenn 1. lediglich die Aufzeichnung nach § 9 Absatz 5 und die nach §§ 11 und 12 vorgeschriebenen Prüfungen und die hierfür notwendige Kommunikation mit der zu identifizierenden Person automatisiert erfolgt und 2. diese Aufzeichnung und das Ergebnis der Überprüfung vor Abschluss des Identifizierungsvorgangs von einem Mitarbeiter detailliert auf Einhaltung der Vorgaben nach §§ 9, 11 und 12 geprüft werden.	Soweit die übrigen Voraussetzungen dieses Abschnitts, **insbesondere bezüglich der audiovisuellen Kommunikation zwischen dem Mitarbeiter und der zu identifizierenden Person,** vorliegen, können teilautomatisierte Verfahren zur Identifizierung Anwendung finden, wenn 1. lediglich die Aufzeichnung nach § 9 Absatz 5 und die nach §§ 11 und **12 (1) und 12 (4)** vorgeschriebenen Prüfungen und die hierfür notwendige Kommunikation mit der zu identifizierenden Person automatisiert erfolgt und 2. diese Aufzeichnung und das Ergebnis der Überprüfung vor **Übermittelung** des Identifizierungsvorgangs **an den Verpflichteten**	Siehe Abschnitt zu § 16 oben.

	von einem Mitarbeiter detailliert auf Einhaltung der Vorgaben nach §§ 9, 11 und 12 geprüft werden.	
§ 17 Einsatz vollautomatisierter Verfahren (1) Bei einem Verfahren, das einen über § 16 hinausgehenden Automatisierungsgrad aufweist, kann eine Eignung zur geldwäscherechtlichen Überprüfung der Identität erprobt werden. Dabei ist zu ermitteln, ob das Verfahren ein Sicherheitsniveau aufweist, das dem nicht-automatisierten Videoidentifizierungsverfahren gleichwertig ist. Die Erprobung kann durch einen Verpflichteten nach § 2 Absatz 1 Nummer 1 GwG oder einem von einem solchen Verpflichteten beauftragten und ermächtigten Dritten erfolgen. (2) Eine Erprobung setzt voraus, dass, 1. das Bundesamt für Sicherheit in der Informationstechnik bei einer zu beantragenden Prüfung des Verfahrens gemessen am aktuellen Stand der Technik ein vergleichbares Sicherheitsniveau zum nicht-automatisierten Videoidentifizierungsverfahren nicht ausgeschlossen hat, und 2. gewährleistet wird, dass das Verfahren keine Anwendung findet für zu identifizierende Personen, bei denen Hinweise auf ein höheres Risiko der Geldwäsche oder Terrorismusfinanzierung gemäß § 15 Absatz 2 GwG vorliegen. Die Prüfung des Verfahrens nach Satz 1 Nummer 1 durch das Bundesamt für Sicherheit in der Informationstechnik hat binnen sechs Monaten nach Beantragung zu erfolgen. (3) Stellt das Bundesamt für Sicherheit in der Informationstechnik zu einem späteren Zeitpunkt fest, dass ein vergleichbares Sicherheitsniveau des Verfahrens zum nicht-automatisierten	(1) Bei einem Verfahren, das einen über § 16 hinausgehenden Automatisierungsgrad aufweist, kann eine Eignung zur geldwäscherechtlichen Überprüfung der Identität erprobt werden **soweit die übrigen Voraussetzungen dieses Abschnitts eingehalten werden**.	Aus unserer Sicht gibt es hier noch sehr viele Unklarheiten und Möglichkeiten diesen Paragrafen auszunutzen.

Videoidentifizierungsverfahren ausgeschlossen ist, darf das Verfahren nicht weiter angewendet werden. Gleiches gilt, wenn Anhaltspunkte dafür bestehen, dass der Verpflichtete die erforderliche Eignung oder Zuverlässigkeit zur dauerhaften Erfüllung der Voraussetzungen dieses Abschnitts nicht hat oder dass der Verpflichtete die Pflichten nach dem Geldwäschegesetz nicht vollständig erfüllt. Gleiches gilt, wenn Anhaltspunkte dafür bestehen, dass der vom Verpflichteten beauftragte Dritte die erforderliche Eignung oder Zuverlässigkeit nicht hat. (4) Die Erprobung darf die Dauer von zwei Jahren nicht überschreiten. Die Verpflichteten haben währenddessen nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik über die Nutzung des zu erprobenden Verfahrens und die dabei gewonnenen Erkenntnisse zu berichten. (5) Spätestens zum Ablauf der Dauer zur Erprobung nach Absatz 4 muss das Verfahren auf Antrag durch das Bundesamt für Sicherheit in der Informationstechnik darauf überprüft werden, ob das Verfahren zur Überprüfung der Identität geeignet ist und ob es ein Sicherheitsniveau aufweist, das dem nicht-automatisierten Videoidentifizierungsverfahren gleichwertig ist. (6) Soweit das Ergebnis der Überprüfung nach Absatz 5 ergibt, dass das Verfahren geeignet ist und ein Sicherheitsniveau aufweist, das dem nicht-automatisierten Videoidentifizierungsverfahren gleichwertig ist, kann das Verfahren ohne weitere Erprobungserfordernisse genutzt werden. Absatz 3 gilt entsprechend.		

§ 18 Aufbewahrung und Aufzeichnung (1) Der gesamte Prozess einer Identifizierung mittels des Videoidentifizierungsverfahrens ist von dem Verpflichteten oder einem Dritten, auf den der Verpflichtete zur Identifizierung gemäß § 17 Absatz 1 und 5 des Geldwäschegesetzes zurückgreift, für die interne und externe Revision sowie für die zuständige Aufsichtsbehörde nachprüfbar in allen Einzelschritten aufzuzeichnen und aufzubewahren. Die Dokumentationspflicht erfordert somit eine visuelle und akustische Aufzeichnung und Aufbewahrung des erfolgten Verfahrensablaufs, auf die sich das Einverständnis der zu identifizierenden Person nach § 8 beziehen muss. (2) Aus den Aufzeichnungen muss neben der Einhaltung der an geldwäscherechtliche Identifizierungen allgemein gestellten Anforderungen insbesondere die Einhaltung der in dieser Verordnung genannten Anforderungen für eine Videoidentifizierung ersichtlich sein. (3) Die Aufzeichnungen sind fünf Jahre aufzubewahren, soweit nicht andere gesetzliche Bestimmungen über Aufzeichnungs- und Aufbewahrungspflichten eine längere Frist vorsehen.		Bitte klarstellen wie dieser Paragraf bei Teilautomatisierung zu deuten ist.
Abschnitt 3 **Datenschutz und Schlussbestimmungen**		
§ 19 Datenschutz Die beteiligten Stellen haben zu gewährleisten, dass bei der Anwendung der in dieser Verordnung geregelten Verfahren die erforderlichen technischen und organisatorischen Maßnahmen nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien		Es sollte klargestellt werden dass eine Datenverarbeitung in der EU zu erfolgen hat.

Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten.		
§ 20 Evaluierung Diese Verordnung ist spätestens drei Jahre nach ihrem Inkrafttreten durch das Bundesministerium der Finanzen im Einvernehmen mit dem Bundesministerium des Innern und für Heimat zu evaluieren. Eine Übernahme der dieser Verordnung zugrunde liegenden Verfahren in andere nationale Rechtsvorschriften lässt die Pflicht zur Evaluierung unberührt.		
§ 21 Inkrafttreten, Außerkrafttreten (1) Diese Verordnung tritt am ersten Tag des auf die Verkündung folgenden Quartals in Kraft und ist auf Videoidentifizierungsverfahren ab dem ersten Tag des auf das Inkrafttreten folgenden Quartals anzuwenden. (2) Diese Verordnung tritt ab dem Zeitpunkt außer Kraft, ab dem unmittelbar anwendbare europäische Regelungen zur Durchführung von geldwäscherechtlichen Sorgfaltspflichten und zu Einzelheiten der dafür erforderlichen Identifizierungsverfahren, einschließlich des Bereichs der Fernidentifizierungsverfahren, anwendbar sind. Der Tag des Außerkrafttretens ist vom Bundesministerium der Finanzen im Bundesgesetzblatt bekannt zu machen.		IDnow ersucht um eine längere Übergangsfrist, um alle technischen Anforderungen umsetzen zu können.

Annex II: Liste der offiziell akzeptierten Dokumente gemäß ANSSI / PVID

Country	Country Name	Document Name	PRADO Reference Code
AD	Andorra	Passport 2017	AND-AO-03001
AE	United Arab Emirates	Passport 2011	UAE-AO-02001
AF	Afghanistan	Passport 2016	AFG-AO-01002
AF	Afghanistan	Passport 2017	AFG-AO-04001
AM	Armenia	Passport 2012	ARM-AO-02001
AO	Angola	Passport 2000	AGO-AO-01001
AR	Argentina	Passport 2012	ARG-AO-03001
AT	Austria	Passport 2006	AUT-AO-02001
AT	Austria	Passport 2014	AUT-AO-02002
AT	Austria	ID Card 2010	AUT-BO-02003
AT	Austria	ID Card 2021	AUT-BO-03001
AT	Austria	Residence Permit 2012	AUT-HO-05001

AT	Austria	Residence Permit 2012	AUT-HO-05002
AT	Austria	Residence Permit 2012	AUT-HO-05003
AT	Austria	Residence Permit 2015	AUT-HO-06001
AT	Austria	Residence Permit 2015	AUT-HO-06002
AT	Austria	Residence Permit 2015	AUT-HO-06003
AT	Austria	Residence Permit 2013	AUT-HO-07001
AT	Austria	Residence Permit 2013	AUT-HO-07002
AT	Austria	Residence Permit 2013	AUT-HO-07003
AT	Austria	Residence Permit 2014	AUT-HO-14001
AT	Austria	Residence Permit 2014	AUT-HO-14002
AU	Australia	Passport 2009	AUS-AO-04001
AU	Australia	Passport 2014	AUS-AO-05001
AZ	Azerbaijan	Passport 2013	AZE-AO-02002
BA	Bosnia and Herzegovina	Passport 2010	BIH-AO-02001

BA	Bosnia and Herzegovina	Passport 2014	BIH-AO-03001
BA	Bosnia and Herzegovina	ID Card 2013	BIH-BO-03001
BD	Bangladesh	Passport 2013	BGD-AO-03001
BE	Belgium	Passport 2008	BEL-AO-07003
BE	Belgium	Passport 2014	BEL-AO-08001
BE	Belgium	Passport 2017	BEL-AO-09003
BE	Belgium	Passport 2019	BEL-AO-10003
BE	Belgium	Passport 2022	BEL-AO-11001
BE	Belgium	Passport 2023	BEL-AO-11002
BE	Belgium	ID Card 2010	BEL-BO-07001
BE	Belgium	ID Card 2010	BEL-BO-08001
BE	Belgium	ID Card 2015	BEL-BO-09001
BE	Belgium	ID Card 2015	BEL-BO-09002
BE	Belgium	ID Card 2015	BEL-BO-09003

BE	Belgium	ID Card 2020	BEL-BO-10001
BE	Belgium	ID Card 2021	BEL-BO-10002
BE	Belgium	ID Card 2021	BEL-BO-11001
BE	Belgium	ID Card 2021	BEL-BO-11004
BE	Belgium	Residence Permit 2013	BEL-HO-08001
BE	Belgium	Resident permit F - flemish	BEL-HO-09001
BE	Belgium	Resident permit F - french	BEL-HO-09002
BE	Belgium	Resident permit F - german	BEL-HO-09003
BE	Belgium	Resident permit F plus - flemish	BEL-HO-10001
BE	Belgium	Resident permit F plus - french	BEL-HO-10002
BE	Belgium	Resident permit F plus - german	BEL-HO-10003
BE	Belgium	Resident permit E - flemish	BEL-HO-11001
BE	Belgium	Resident permit E - french	BEL-HO-11002
BE	Belgium	Resident permit E - german	BEL-HO-11003

BE	Belgium	Resident permit E plus - flemish	BEL-HO-12001
BE	Belgium	Resident permit E plus - french	BEL-HO-12002
BE	Belgium	Resident permit E plus - german	BEL-HO-12003
BF	Burkina Faso	Passport 2013	BFA-AO-03001
BG	Bulgaria	Passport 2010	BGR-AO-02001
BG	Bulgaria	ID Card 2010	BGR-BO-02001
BI	Burundi	Passport 2018	BDI-AO-02001
BR	Brazil	Passport 2010	BRA-AO-02001
CA	Canada	Passport 2013	CAN-AO-04001
CH	Switzerland	Passport 2010	CHE-AO-03002
CH	Switzerland	Passport 2022	CHE-AO-04001
CH	Switzerland	ID Card 2005	CHE-BO-01003
CH	Switzerland	ID Card 2023	CHE-BO-02001
CI	Cote d'Ivoire	Passport 2008	CIV-AO-02001

CN	China	Hong Kong 2007	CHN-AO-03003
CN	China	Hong Kong 2019	CHN-AO-03004
CN	China	Macao 2009	CHN-AO-04003
CN	China	Passport 2012	CHN-AO-05001
CO	Colombia	Passport 2010	COL-AO-02001
CO	Colombia	Passport 2019	COL-AO-04001
CY	Cyprus	Passport 2009	CYP-AO-04001
CY	Cyprus	ID Card 2015	CYP-BO-04001
CY	Cyprus	ID Card 2020	CYP-BO-04002
CY	Cyprus	Residence Permit 2020	CYP-HO-05001
CZ	Czech Republic	Passport 2006	CZE-AO-04001
CZ	Czech Republic	ID Card 2012	CZE-BO-04001
CZ	Czech Republic	ID Card 2014	CZE-BO-04002
CZ	Czech Republic	ID Card 2021	CZE-BO-04003

DE	Germany	Passport 2007	DEU-AO-01006
DE	Germany	Passport 2007	DEU-AO-01007
DE	Germany	Passport 2017	DEU-AO-04001
DE	Germany	ID Card 2010	DEU-BO-02001
DE	Germany	ID Card 2021	DEU-BO-02004
DE	Germany	Residence Permit 2011	DEU-HO-21001
DE	Germany	Residence Permit 2011	DEU-HO-21002
DE	Germany	Residence Permit 2011	DEU-HO-21003
DE	Germany	Residence Permit 2019	DEU-HO-22003
DE	Germany	Residence Permit 2021	DEU-HO-22005
DJ	Djibouti	Passport DJI 2017	DJI-AO-02001
DK	Denmark	Passport 2004	DKN-AO-04001
DK	Denmark	Passport 2004	DKN-AO-05001
DK	Denmark	Passport 2004	DKN-AO-05002

DK	Denmark	Passport 2004	DKN-AO-05003
DK	Denmark	Passport 2004	DNK-AO-03001
DK	Denmark	Passport 2020	DNK-AO-06001
DZ	Algeria	Passport 2012	DZA-AO-01001
EE	Estonia	Passport 2007	EST-AO-02005
EE	Estonia	Passport 2014	EST-AO-03005
EE	Estonia	Passport 2021	EST-AO-06001
EE	Estonia	ID Card 2011	EST-BO-03001
EE	Estonia	ID Card 2018	EST-BO-04001
EE	Estonia	ID Card 2021	EST-BO-04002
EG	Egypt	Passport 2008	EGY-AO-01001
ES	Spain	Passport 2006	ESP-AO-04001
ES	Spain	Passport 2015	ESP-AO-05001
ES	Spain	ID Card 2006	ESP-BO-03001

ES	Spain	ID Card 2015	ESP-BO-05001
ES	Spain	ID Card 2021	ESP-BO-06001
ES	Spain	Residence Permit 2011	ESP-HO-02005
ES	Spain	Residence Permit 2020	ESP-HO-03001
FI	Finland	Passport 2012	FIN-AO-05001
FI	Finland	Passport 2012	FIN-AO-05002
FI	Finland	Passport 2017	FIN-AO-06001
FI	Finland	Passport 2023	FIN-AO-07001
FI	Finland	Passport 2023	FIN-AO-07002
FI	Finland	ID Card 2011	FIN-BO-06001
FI	Finland	ID Card 2017	FIN-BO-09001
FI	Finland	ID Card 2021	FIN-BO-11001
FI	Finland	ID Card 2023	FIN-BO-12001
FI	Finland	ID Card 2023	FIN-BO-12004

FI	Finland	Minors ID Card 2017	FIN-BO-10001
FR	France	Passport 2013	FRA-AO-03003
FR	France	Passport 2019	FRA-AO-03004
FR	France	ID Card 1994	FRA-BO-02002
FR	France	ID Card 2021	FRA-BO-03001
FR	France	Residence Permit 2011	FRA-HO-09001
FR	France	Residence Permit 2020	FRA-HO-12001
GB	United Kingdom	Passport 2010	GBR-AO-04001
GB	United Kingdom	Passport 2015	GBR-AO-05001
GB	United Kingdom	Passport 2020	GBR-AO-06001
GE	Georgia	ID Card 2011	GEO-BO-01001
GH	Ghana	Passport 2010	GHA-AO-02001
GN	Guinea	Passport 2018	GIN-AO-03001
GR	Greece	Passport 2006	GRC-AO-03001

GR	Greece	Passport 2006	GRC-AO-03002
GR	Greece	Passport 2006	GRC-AO-03003
HR	Croatia	Passport 2009	HRV-AO-02001
HR	Croatia	ID Card 2003	HRV-BO-02001
HR	Croatia	ID Card 2013	HRV-BO-03001
HR	Croatia	ID Card 2015	HRV-BO-03002
HR	Croatia	ID Card 2021	HRV-BO-04001
HU	Hungary	ID Card 2012 - B	HUN-BO-04001
HU	Hungary	ID Card 2012 - A	HUN-BO-04002
HU	Hungary	ID Card 2016	HUN-BO-05001
HU	Hungary	ID Card 2016	HUN-BO-05002
HU	Hungary	ID Card 2016	HUN-BO-05003
HU	Hungary	ID Card 2016	HUN-BO-05004
IE	Ireland	Passport 2013 - B	IRL-AO-04002

IE	Ireland	Passport 2013 - A	IRL-AO-05001
IE	Ireland	ID Card 2015	IRL-TO-01002
IL	Israel	Passport 2012	ISR-AO-03001
IR	Islamic Republic of Iran	Passport 2014	IRN-AO-04001
IS	Iceland	Passport 2006	ISL-AO-03001
IS	Iceland	Passport 2019	ISL-AO-05001
IT	Italy	Passport 2010	ITA-AO-02004
IT	Italy	ID Card 2016	ITA-BO-04004
IT	Italy	ID Card 2022	ITA-BO-04005
JP	Japan	Passport 2013	JPN-AO-02003
JP	Japan	Passport 2013	JPN-AO-02004
KE	Kenya	Passport 2015	KEN-AO-03001
KR	Korea (South)	Passport 2008	KOR-AO-03002
KR	Korea (South)	Passport 2021	KOR-AO-04001

KW	Kuwait	Passport 2016	KWT-AO-01001
KZ	Kazakhstan	Passport 2010	KAZ-AO-02001
LB	Lebanon	Passport 2016	LBN-AO-02001
LI	Liechtenstein	ID Card 2009	LIE-BO-02001
LT	Lithuania	Passport 2008	LTU-AO-04001
LT	Lithuania	Passport 2008	LTU-AO-04002
LT	Lithuania	Passport 2008	LTU-AO-04003
LT	Lithuania	Passport 2019	LTU-AO-04004
LU	Luxembourg	Passport 2006	LUX-AO-02003
LU	Luxembourg	Passport 2015	LUX-AO-02005
LU	Luxembourg	Passport 2006	LUX-AO-03001
LV	Latvia	ID Card 2012	LVA-BO-01001
LV	Latvia	ID Card 2019	LVA-BO-02001
LY	Libya	Passport 2013	LBY-AO-02001

MA	Morocco	Passport 2009	MAR-AO-02001
MC	Monaco	ID Card 2009	MCO-BO-01001
MD	Moldova	Passport 2014	MDA-AO-01004
MD	Moldova	Passport 2018	MDA-AO-05001
MD	Moldova	ID Card 2015	MDA-BO-02001
MD	Moldova	ID Card 2015	MDA-BO-02002
ME	Montenegro	Passport 2008	MNE-AO-02001
MK	Macedonia	Passport 2007	MKD-AO-03001
ML	Mali	Passport 2007	MLI-AO-02001
ML	Mali	Passport 2016	MLI-AO-03002
MR	Mauritania	Passport 2013	MRT-AO-01001
MT	Malta	Passport 2008	MLT-AO-04001
MT	Malta	ID Card 2002	MLT-BO-02001
MT	Malta	ID Card 2014	MLT-BO-03001

MV	Maldives	Passport 2016	MDV-AO-04001
MW	Malawi	Passport 2011	MWI-AO-02001
MX	Mexico	Passport 2016	MEX-AO-03001
MX	Mexico	Passport 2012	MEX-AO-02004
MY	Malaysia	Passport 2010	MYS-AO-02001
MY	Malaysia	Passport 2017	MYS-AO-03001
NG	Nigeria	Passport 2019	NGA-AO-03001
NL	Netherlands	Passport 2011	NLD-AO-03001
NL	Netherlands	Passport 2014	NLD-AO-04001
NL	Netherlands	Passport 2021	NLD-AO-05001
NL	Netherlands	ID Card 2014	NLD-BO-04001
NL	Netherlands	ID Card 2017	NLD-BO-05001
NL	Netherlands	ID Card 2021	NLD-BO-06001
NL	Netherlands	ID Card 2021	NLD-BO-07001

NO	Norway	Passport 2011	NOR-AO-04001
NO	Norway	Passport 2011	NOR-AO-05001
NO	Norway	Passport 2020	NOR-AO-06001
NZ	New Zealand	Passport 2009	NZL-AO-03002
NZ	New Zealand	Passport 2021	NZL-AO-04001
PE	Peru	Passport 2016	PER-AO-02001
PH	Philippines	Passport 2010	PHL-AO-02001
PH	Philippines	Passport 2010	PHL-AO-03001
PH	Philippines	Passport 2016	PHL-AO-04001
PL	Poland	Passport 2006 - B	POL-AO-04001
PL	Poland	Passport 2006 - A	POL-AO-05001
PL	Poland	Passport 2018	POL-AO-06001
PL	Poland	Passport 2022	POL-AO-07001
PL	Poland	ID Card 2001-2013	POL-BO-02001

PL	Poland	ID Card 2001-2013	POL-BO-02002
PL	Poland	ID Card 2001-2013	POL-BO-02003
PL	Poland	ID Card 2015	POL-BO-03001
PL	Poland	ID Card 2019	POL-BO-04001
PL	Poland	ID Card 2021	POL-BO-05001
PL	Poland	Residence Permit 2014	POL-HO-11002
PL	Poland	Residence Permit 2020	POL-HO-12001
PT	Portugal	Passport 2009	PRT-AO-01003
PT	Portugal	Passport 2017	PRT-AO-04001
PT	Portugal	ID Card 2015	PRT-BO-03005
PT	Portugal	Residence Permit 2008	PRT-HO-02001
PT	Portugal	Residence Permit 2019	PRT-HO-06001
RO	Romania	Passport 2019	ROU-AO-03001
RO	Romania	ID Card 2021	ROU-BO-05001

RS	Serbia	Passport 2008	SRB-AO-01001
RU	Russian Federation	Passport 2010	RUS-AO-03003
RW	Rwanda	Passport 2019	RWA-AO-02001
SE	Sweden	Passport 2012	SWE-AO-04001
SE	Sweden	Passport 2022	SWE-AO-05001
SE	Sweden	ID Card 2012	SWE-BO-03001
SE	Sweden	ID Card 2021	SWE-BO-03002
SE	Sweden	ID Card 2022	SWE-BO-04001
SE	Sweden	Residence Permit 2012	SWE-HO-09001
SG	Singapore	Passport 2006	SGP-AO-04001
SG	Singapore	Passport 2017	SGP-AO-05001
SI	Slovenia	Passport 2006	SVN-AO-02001
SI	Slovenia	Passport 2006	SVN-AO-02002
SI	Slovenia	Passport 2006	SVN-AO-02003

SI	Slovenia	Passport 2016	SVN-AO-02004
SI	Slovenia	ID Card 1998	SVN-BO-02001
SK	Slovakia	Passport 2008	SVK-AO-03001
SK	Slovakia	Passport 2014	SVK-AO-04001
SK	Slovakia	ID Card 2013	SVK-BO-03001
SK	Slovakia	ID Card 2013	SVK-BO-04001
SK	Slovakia	ID Card 2015	SVK-BO-05001
TH	Thailand	Passport 2012	THA-AO-02002
TH	Thailand	Passport 2020	THA-AO-06001
TR	Turkey	Passport 2010	TUR-AO-02001
TR	Turkey	Passport 2017	TUR-AO-03001
TW	Taiwan	Passport 2008	TWN-AO-03001
TW	Taiwan	Passport 2018	TWN-AO-04001
TW	Taiwan	Passport 2018	TWN-AO-04002

UA	Ukraine	Passport 2007	UKR-AO-02001
UA	Ukraine	Passport 2007	UKR-AO-02002
UA	Ukraine	Passport 2015	UKR-AO-03001
UA	Ukraine	Passport 2015	UKR-AO-03002
UA	Ukraine	ID Card 2016	UKR-BO-2016
US	United States of America	Passport 2006	USA-AO-04001
US	United States of America	Passport 2020	USA-AO-05001
VE	Venezuela	Passport 2011	VEN-AO-02001
XK	Kosovo	Passport 2013	RKS-AO-03001
XK	Kosovo	ID Card 2013	RKS-BO-02001
ZA	South Africa	Passport 2009	ZAF-AO-02001