Stellungnahme

Anhörung zur Neugestaltung der Verfügung gemäß § 111 Absatz 1 Satz 4 Telekommunikationsgesetz

15. Juni 2021

Zusammenfassung

Ansprechpartner

Maximilian Wiemer
Referent für Recht und Regulierung
VATM e.V.
Frankenwerft 35
50667 Köln
Tel. +49 221 / 37677 33
E-Mail: mw@vatm.de
www.vatm.de

Nick Kriegeskotte
Leiter Infrastruktur & Regulierung
Bitkom e.V.
Albrechtstraße 10
10117 Berlin
Tel. +49 30 27576-224
E-Mail: n.kriegeskotte@bitkom.org
www.bitkom.org

Die Branchenverbände Bitkom und VATM begrüßen die Anhörung der betroffenen Kreise im Rahmen der Einführung alternativer Identifizierungsverfahren gem. § 111 TKG und möchten hierzu gerne wie Folgt Stellung nehmen.

Außerhalb des Fragenkatalogs möchten wir darauf aufmerksam machen, dass es seitens der Branche grundsätzlich als erschwerend empfunden wird, dass die Anerkennung eines Identifizierungsverfahrens gem. § 172 Abs. 2 TKG (2021) künftig nur noch unter Einbeziehung einer Konformitätsbewertungsstelle möglich sein wird, da dies zu zusätzlichen bürokratischen Aufwänden führt und fraglich erscheint, ob für den Anwendungsfall der Verifizierung von Prepaid-Anschlussinhaberdaten eine ausreichende Fallzahl für eine Prüfung durch Konformitätsstellen erreicht werden kann.

Aus Sicht der Branche bestehen daher im Grundsatz zwei Möglichkeiten bis zum Inkrafttreten des neuen TKG: Einerseits könnte die Verpflichtung zur Validierung der Anschlussinhaberdaten bei den Mobilfunkunternehmen für den Fall verbleiben, dass diese Verfahren einsetzen, die nicht von einer Konformitätsbewertungsstelle geprüft worden sind. Andererseits könnte die Verpflichtung bei bereits akkreditierten Verfahren auf diese übertragen werden.

In jedem Fall sollte von den öffentlichen Stellen ein Prüfset mit Musterdaten zur Verfügung gestellt werden, um die Akkreditierungsschritte nachzuvollziehen und zu prüfen.

Während wir ebenfalls denken, dass eine zu hohe Bürokratie der Innovation unnötige Steine in den Weg legen kann, hat sich das System der Konformitätsbewertungsstellen für Vertrauensdienste bewährt. Wir sind der Meinung, dass eine akkreditierte Instanz das nötige Vertrauen in die Leistungsfähigkeit des Systems bringen kann, was wiederum die Einführung eines Systems bei TK-Unternehmen vereinfacht, da diese weniger Prüfaufwände hätten und sich nicht nur auf die Aussagen eines Anbieters verlassen müssten. Allgemein sind Zertifizierungen im IT-Sicherheitsbereich als üblich anzusehen und in den

überwiegenden Fällen nicht als schädlich zu betrachten. Aus Sicht der Branche stellt sich allerdings die Frage wer die Konfirmitätsbewertungsstellen benennt.

Die nachfolgende Stellungnahme möchten wir ungeachtet dessen dazu nutzen, der Bundesnetzagentur einen Überblick über die modernen Methoden der Personenidentifizierung und Dokumentenverifizierung vor allem unter Einsatz künstlicher Intelligenz zu geben, um damit darzulegen, dass vor allem die sich aus dem Kriterienkatalog des Referats IS15 ergebenden Anforderungen nicht den aktuellen Stand der Technik berücksichtigen und demnach erst recht im Bereich der Identifizierung von Prepaid-Telekommunikationskunden keinen angemessenen und erforderlichen Maßstab bilden.

Wir möchten daher zunächst allgemein zu dem Kriterienkatalog des Referates IS15 und dem daraus erkennbaren Verständnis der aktuellen Verfahren zur automatisierten Identifizierung von Personen und Dokumentenerkennung Stellung nehmen.

Aus der Verfügung der BNetzA zur vorläufigen Anerkennung einer innovativen Identifizierungsmethode gem. § 11 Abs. 3 VDG vom April 2021 ergeben sich aus Sicht der Industrie Fragestellungen zu Formulierungen. Es stellt sich die Frage welcher Sinn und Zweck erreicht werden soll, bevor die Umsetzbarkeit überhaupt bewertet werden kann. Beispielhaft sei hier der erforderliche „Videostream“ genannt, der technisch auch als nicht-live Stream ausgestaltet werden sollte, um auch eine Verifizierungsmöglichkeit bei schwächeren Internetverbindungen zu ermöglichen. Vorgaben müssen zudem so ausgestaltet sein, dass sie einem Nutzerverständnis zugänglich sind. Dies ist bei Vorgaben wie dem „Finger vorhalten“, welche sich aus dem VideoIdent-Verfahren ableiten, nicht gegeben. Im Ergebnis müssen die Vorgaben so ausgestaltet werden, dass sie technisch umsetzbar und verbraucherfreundlich nutzbar sind.

Es soll an dieser Stelle nur kursorisch auf die Kernpunkte der veröffentlichten Verfügung eingegangen werden:

1. Bezugnahme auf ETSI Normen

Die Bezugnahme auf die ETSI Normen zur risikoorientierten technischen Umsetzung von Identifikations- und Authentifikationsprozessen bei Vertrauensdiensten wird grundsätzlich begrüßt. Die genannten ETSI Regeln bilden den technisch-prozessualen Standard der europäischen Vertrauensdiensteregulierung über die eIDAS Verordnung ab und dienen als solche als Richtschnur für die Übereinstimmung von Identifikationsverfahren nach europäischen Vorgaben.

Kernelement der eIDAS Verordnung ist aber gerade ein technikoffener, risikobasierter Ansatz.

Danach sind bei unterschiedlichen Vertrauensniveaus unterschiedliche Identifizierungssysteme zulässig. Vorgaben zur konkreten Umsetzung durch ein bestimmtes Verfahren macht die eIDAS Verordnung aber nicht, und aus diesem Grund sind in den meisten europäischen Ländern mit der Ausnahme von Deutschland, auch Auto-Identverfahren (z.B. auch im Bereich der Geldwäscheprävention) möglich, solange sie ein dem persönlichen Vorsprechen der zu identifizierenden Person vergleichbares Sicherheitsniveau anbieten und von der prüfenden Stelle (z.B. der Bank) nach Durchführung einer Risikoanalyse als ausreichend betrachtet werden.

Allein Deutschland gibt mit den sehr restriktiven Vorgaben für zulässige Identifizierungsverfahren ein technisches Verfahren von Regulierungsseite ex ante vor, anstatt wie die meisten anderen Mitgliedsstaaten basierend auf der konkreten Risikoanalyse dem technikoffenen Ansatz zu vertrauen.

Vor diesem Hintergrund wären die Anforderungen der ETSI Normen im Zusammenhang mit einer Konformitätsbewertung nach ETSI auch für Deutschland ein hinreichender Anknüpfungspunkt gewesen und es hätte grundsätzlich der weiteren Anforderungen der Verfügung nicht bedurft.

Allerdings befindet sich die ETSI Richtlinie für Identitätsfeststellungsverfahren noch im Draft, weshalb das Zurückgreifen im Bereich der Vertrauensdiensteregulierung auf die ergänzenden Kriterien zum VDG der BNetzA im Einvernehmen mit dem BSI aktuell als sinnvoll erscheint.

2. Allgemeine und konkrete Anforderungen an das alternative Verfahren

Die Industrie kann grundsätzlich die von der BNetzA vorgegebenen allgemeinen Anforderungen in Bezug auf Manipulationsvermeidung, Echtzeitkontrolle, Verschlüsselung, Bild- und Videoqualität und deren Überprüfung nachvollziehen. Auch ist die Nutzung hinreichend prüfbarer Identitätsdokumente und von deren Sicherheitsmerkmalen und die Anforderungen an deren Überprüfung nachvollziehbar und sinnvoll.

Allerdings verwundert die Bezugnahme auf den Begriff des „Videostreams“. Ein Automatisiertes Verfahren kann nur mit verschiedenen technischen Komponenten, die nacheinander in einer zeitlichen Abfolge abzuarbeiten sind, durchgeführt werden. Ein durchgehender Videostream, wie dieser beim Video-Ident-Prozess vom Beginn des Videotelefonats bis zu dessen Abschluss stattfindet, ist nicht nur kaum möglich, da er bedeuten würde, dass der Bildschirm des Nutzers aufgezeichnet werden müsste, noch erlaubt ein solches einheitliches Verfahren den hinreichend sicheren Einsatz der Komponenten: Ein Auto-Identverfahren besteht im Wesentlichen aus 4 typischen Schritten, denen jeweils ggf. noch Interaktivitätselemente hinzugefügt werden können: 1. Aufnahme des abzugleichenden Personaldokuments von beiden Seiten 2. Verarbeitung der eingelesenen Daten, insb. des Fotos zum Zweck des nachfolgenden Abgleichs, Echtheits- und Plausibilitätsprüfung anhand der eingelesenen Daten und Bilddaten, 3. Aufnahme eines Selfievideos zum nachfolgenden Abgleich mit dem vom Dokument extrahierten Foto, 4. Bindung des Dokumentes an den Nutzer z.B. durch Abgleich mit anderen Datenquellen (Adressdatenbanken, Bankdaten) sowie dem Abgleich von Dokumentenfoto mit Selfievideo.

Optional kann auch noch ein interaktives Element hinzugefügt werden, um die Authentizität des jeweiligen Nutzers zum Zeitpunkt der Durchführung des Identifikationszeitpunkts zu gewährleisten (Gleichzeitigkeit).

Die Aufnahme eines Videostreams ist daher nicht nur nicht erforderlich, um den ununterbrochenen Identifizierungsvorgang zu gewährleisten, sie stellt auch einen unangemessenen Eingriff in die Privatsphäre des Nutzers da, wenn dessen Displayanzeige aufgezeichnet werden sollte. Allerdings ist hier aktuell noch nicht ersichtlich beschrieben, wie die Aktualität der Aufnahme gewährleistet wird und nicht beispielsweise ein voraufgenommenes Video / Foto in den Prozess eingespielt wird. Dies ist letztendlich unserer Einsicht nach die Anforderung, die mit dem Begriff “Videostream” erreicht werden soll.

Aus den ergänzenden Kriterien der BNetzA ergeben sich zusätzlich noch Vorgaben zum Verfahren der Überprüfung der Dokumentenechtheit. Auch hier werden typische, ausschließlich für einen Videocall anwendbare Verfahren, wie das Abdecken von Elementen mit den Fingern gefordert. Die Forderung nach interaktiven Elementen ist durchaus nachvollziehbar und sinnvoll, deren konkrete Umsetzung sollte allerdings dem Anbieter anhand der technischen Gegebenheiten überlassen werden. In einem automatisierten Verfahren dürften z.B. Verfahren mit Abdeckung von Elementen eher zu Prüfungenauigkeiten führen. Sie sind im automatisierten Verfahren aber auch nicht erforderlich, weil die KI gestützte Dokumentenprüfung durch weitaus weiter entwickelte Techniken dazu in der Lage ist, anhand der Frames einer

Dokumentenaufnahme die Sicherheitsfeatures eines Dokumentes zu erkennen. Das Abdecken zum Beispiel macht hingegen nur beim Einsatz eines menschlichen Operators Sinn, dem die Techniken der künstlichen Intelligenz, die zur Dokumentenanalyse beim automatisierten Verfahren herangezogen werden können, nicht zur Verfügung stehen.

Damit sind an dieser Stelle nur die signifikantesten Probleme der Verfügung beschrieben. Diese sind aber kennzeichnend für den heutigen Stand der Technik und sollten daher dringend auch von der Bundesnetzagentur und dem BSI zur Beurteilung der Eignung herangezogen werden. Die Industrie bietet hierzu gerne umfassende Darlegungen zum technischen Stand und dessen Geeignetheit und Sicherheit auch im Zusammenhang mit Vertrauensdiensten an.

Letztlich sind auch die sehr strengen Vorgaben des BfDI bezüglich der Daten zum Zwecke der Auswertung im Rahmen des machine learnings zu überdenken.

Die Genauigkeit der KI-Engines hängt stark von der Anzahl und der Diversität der zur Verfügung stehenden Daten ab, die dazu dienen, die Engine in einer kontinuierlichen Weise zu trainieren.

Die AutoIdent- und Videoidentifikation ermöglicht nichtdeutschen EU-Inländern die Teilnahme am digitalen Leben in Deutschland, da sie in Bezug auf die Staatsangehörigkeit diskriminierungsfrei genutzt werden kann. Zum jetzigen Zeitpunkt hat nicht jeder EU-Mitgliedstaat Ausweise mit einer elektronischen Identitätsfunktion im Umlauf. Die vorhandenen Systeme anderer Mitgliedstaaten sind zudem nicht immer mit der deutschen eID vergleichbar. Für nichteuropäische Kunden ist der Aufwand des Zugangs zu einer notifizierten eIDLösung zudem als zu hoch anzusehen.

Sicherheitsbedenken müssen adressiert werden, dürfen aber den Marktzugang sowie die Praktikabilität digitaler Transaktionen nicht verstellen und sollten sich stets an den Praxiserfahrungen orientieren. Die Videoidentifikation ist nicht unsicherer als andere, derzeit genutzte Verfahren. Das Sicherheitsniveau der Videoidentifikation ist zudem bereits als sehr hoch einzustufen.

Zudem wird angeregt, die Weiterverwendungsmöglichkeit von durch geldwäscherechtlich verpflichtete Unternehmen erhobene Identifikationsdaten im TKG-Kontext einerseits zu erweitern sowie andererseits zu konkretisieren.

Des Weiteren möchten wir an dieser Stelle auf das aktuell vom Bundeskanzleramt vorangetriebene Projekt aufmerksam machen, in dem zum einen die Personalausweisdaten in einer Wallet-App auf dem Mobiltelefon gespeichert werden sollen und zum anderen die Basis-ID auch für Vertragsabschluss von Prepaid-Telekommunikationsverträgen genutzt werden soll. Die festzulegenden Regelungen zu § 111 TKG sollten dieses Projekt – neben KI gestützten Autoidentverfahren - mit im Blick haben und nicht erschweren oder unmöglich machen, da es aufgrund der Erwartungen des Kanzleramtes mit erheblichen Aufwand für die Mobilfunknetzbetreiber verbunden ist und daher keine „Eintragsfliege“ sein sollte.

Dies vorausgeschickt, gehen wir im Folgenden auf die einzelnen Fragen des veröffentlichten Fragenkatalogs näher ein:

Zum Fragenkatalog

1. ***Die Verfälschung von Videostreams (z. B. mittels sog. „Deepfakes“) ermöglicht mit relativ einfachen Mitteln das VideoIdent-Verfahren zu manipulieren:***

    a. *Wie bewerten Sie das resultierende Gefährdungspotential?*

Rechtssichere Verfahren zur Identifizierung von Geschäftspartnern sind für die sichere und vertrauensgesicherte Durchführung von digitalen Geschäftsprozessen unerlässlich. Immer mehr Dienste, auch grenzüberschreitender Art, benötigen ein hohes Maß an Identifizierungssicherheit. Videoidentifizierung wird deswegen bereits sehr erfolgreich in den Anwendungsbereichen des Telekommunikationsgesetzes (TKG) und des Geldwäschegesetzes (GWG) eingesetzt. Für Banken und Telekommunikationsanbieter sind Identifizierungsdienstleister integraler Bestandteil der Schutzmechanismen zur Verhinderung von Terrorismusfinanzierung, Geldwäsche und organisierter Kriminalität.

Außerhalb von Labor-Versuchen sind uns in der Praxis jedoch keine Fälle bekannt, bei denen Verfälschung von Videostreams (z. B. mittels sog. „Deepfakes“) im Rahmen von Video-Identverfahren stattgefunden haben.

Verfälschungen von Videostreams erfordern auf Seiten des Angreifers zunehmend umfassendes Wissen und hohen technischen Aufwand, so dass angesichts der Tatsache, dass es auch zahlreiche andere Möglichkeiten gibt, sich „anonyme“ SIM-Karten (sei es über Online-Plattformen oder aus dem Ausland) zu besorgen, kaum wahrscheinlich ist, dass im Bereich der Prepaidkartenregistrierung hier signifikant messbare Betrugsversuche unternommen werden. Deep-Fakes oder andere Betrugsversuche, wie Maskenattacken oder Nötigungssituationen sind dennoch auch im Video-Identverfahren nicht ganz auszuschließen und im Zweifel durch einen menschlichen Operator auch nicht immer zuverlässig zu erkennen. Technische Lösungen im Zusammenhang mit künstlicher Intelligenz hingegen bieten Ansätze, solche Betrugsversuche erkennbar zu machen, und werden im Rahmen der Weiterentwicklung von Identifizierungsdiensten eine zunehmende Rolle einnehmen.

Erfahrungen bei Telekommunikationsidentifizierung in der Schweiz zeigen, dass mit Einführung eines automatisierten Verfahrens Betrugsversuche bei der Registrierung von SIM-Karten im Vergleich zu den vorherigen Verfahren und im Vergleich zu Betrugsversuchen im stationären Handel sogar stark abgenommen haben. Betrüger fürchten die Kontaktaufnahme über einen Online-Prozess, der neben der Aufnahme von Fotos und Videos auch die Erhebung von Metadaten der Verbindung ermöglicht und so eine Ermittlung eines Betrügers eher noch wahrscheinlicher werden lässt. Jedenfalls können die Schweizer Mobilfunkanbieter von keinerlei erhöhtem Risiko in diesem Sinne berichten.

Im Ergebnis ist das Gefährdungspotenzial vor allem im Zusammenspiel mit den im Rahmen der nächsten Frage dargestellten Gegenmaßnahmen als äußerst niedrig einzustufen.

    b. *Welche Vorkehrungen/Maßnahmen können diesem Gefährdungspotential entgegenwirken und werden diese bereits umgesetzt?*

Zur Verhinderung von Manipulationen des Videobildes werden bei den bereits in der Praxis angewendeten Auto-Identverfahren verschiedene Kontrollmechanismen eingesetzt, die bereits heute zuverlässig in der Lage sind, Betrugsversuche zu erkennen.

Eine Kernfunktionalität ist hierbei die so genannte „Liveness Detection". Diese ist sowohl aktiv möglich, also durch das Einbinden interaktiver Handlungsanweisungen (wie Kopf nach links oder rechts drehen) als auch passiv unter Einsatz von Techniken der künstlichen Intelligenz.

Liveness Detection-Lösungen helfen, das Fraud-Problem zu lösen, indem festgestellt wird, ob sich eine reale Person vor der Kamera befindet. Dies ist entscheidend für die Gewährleistung eines sicheren und genauen Identitätsprüfungssystems. Passive Liveness Detection erschwert es Betrügern, das System mit 3D-gescannten Masken, Papierfotos, Deep-Fakes und anderen Objekten, die für Präsentationsangriffe verwendet werden, zu fälschen.

Passive Liveness Detection basiert auf biometischen Daten. Der Hauptbestandteil besteht darin, dass sie mithilfe von Computer Vision- und Deep-Learning-Algorithmen „Lebendigkeit" oder „Präsenz" in einer Person erkennt - etwas, das weit über das allgemeine Konzept der Gesichtsüberprüfung hinausgeht.

Während bei der herkömmlichen Gesichtsüberprüfung nur festgestellt wird, dass das Gesicht vor der Kamera einem anderen, möglicherweise bereits registrierten Gesicht entspricht, wird durch die Lebendigkeitserkennung geklärt, ob eine reale, lebende Person vorhanden ist oder ob die Daten von einem leblosen Objekt stammen. Daneben können Deep-Fakes auch maschinell anhand der unterschiedlichen Codierungen aufgezeichneter oder live aufgenommener Videos erkannt werden.

Setzt man neben der passiven Liveness Detection ggf. noch ein zusätzliches interaktives Element (wie eine Interaktion auf dem Endgerät) ein, entsteht ein hoch sicherer Identifizierungsprozess, der selbst die Kontrolle unter anwesenden Personen erheblich übersteigt.

Eine weitere Methode zur Minimierung des Gefährdungspotentials sind technische Verfahren zur Sicherung der Aktualität der Aufnahmen. Damit wird effektiv verhindert, dass voraufgenommene Dateien eingespielt werden, die ggf. manipuliert oder gestohlen sind (Identitätsdiebstahl). (Labor)angriffe auf Video-Ident fanden bisher meist mit einer sogenannten Fake-Webcam statt, um vorab manipulierte Dateien einzuspielen (asynchrone Manipulation) oder gar eine live Manipulation (synchrone Manipulation) des Streams durchzuführen. Dies wird durch eine effektive Methode zur Sicherung der Aktualität der Aufnahmen soweit erschwert, dass es aktuell kein wirtschaftlich sinnvoller Angriff ist, einen Deep-Fake durchzuführen, sondern lieber den Weg über eine offline Filiale zu gehen.

2. Teil- oder vollautomatisierte Verifikationslösungen

a. *Wird der Einsatz teil- oder vollautomatisierter Verifikationslösungen zur Identifikation gemäß § 111 TKG erwogen, ähnlich den im Bereich der elektronischen Vertrauensdienste jüngst vorläufig anerkannten Verfahren (https://www.elektronische-vertrauensdienste.de/EVD/SharedDocuments/Downloads/QES/VerfuegungIdentmethoden/VerfuegungAutoIdent2021.pdf)?*

Der Einsatz kommt für Telekommunikationsdienste in Betracht, sofern sich diese als sicher erweisen, die Implementierung mit angemessenem Aufwand erfolgen kann und eine einzelne Datenprüfung kostengünstig angeboten werden kann.

Von einem automatisierten Verifikationsverfahren wären insbesondere folgende Vorteile zu erwarten:

1. Sicherheit

a) Der Prozess bei einem teil- oder vollautomatisierten Verfahren könnte eine höhere Sicherheit aufweisen. Denn Künstliche Intelligenz dürfte im Vergleich zu menschlichen Prüfern geeigneter und präziser sein für die Prüfung hunderter Ausweisdokumente.

b) Dies gilt insbesondere für ausländische Ausweisdokumente und sonstige Sonderfälle. Hier hat sich gezeigt, dass auch bei intensiver Schulung menschliche Fehler unterlaufen bzw. es nicht möglich ist, adäquat auf Authentizität zu prüfen.

2. Kundenfreundlichkeit

a) Erfahrungsgemäß besteht bei vielen Kunden die Befürchtung eines Missbrauchspotentials, wenn menschliche Agenten involviert sind. In einen Prozess ohne Übermittlung von Ausweisdaten an einen menschlichen Agent könnte daher ein größeres Vertrauen bestehen.

b) Sprachbarrieren könnten beseitigt werden. Häufig bestehen Verständnisprobleme durch schlecht oder kein Deutsch sprechende Kunden und/oder Agenten. Ein digitaler Prozess könnte sich zum einen durch einfache Anweisungen auszeichnen, zudem einfacherer in mehreren Sprachen ausgestaltet werden.

c) Ein komplett digitalisierter Prozess wäre nicht an die Geschäftszeiten gebunden. Daraus ergibt sich mehr Flexibilität für den Kunden.

d) Die Anforderungen an die Daten-Verbindung dürften geringer sein. Darauf folgt die Hoffnung, dass aus Kundensicht weniger Abbrüche geschehen, da geringerer Datenverbrauch/weniger Bandbreite erforderlich als bei einem Live-Videochat.

b. Bestehen Bedenken gegen das Anlegen der im Bereich der elektronischen Vertrauensdienste entwickelten Maßstäbe auch für Identifizierungsverfahren gemäß § 111 TKG?

Entscheidend ist aus Sicht der Branche eine europaweit einheitliche Handhabung elektronischer Vertrauensdienste, die nicht durch unterschiedliche nationale Anwendungsvorgaben konterkariert wird. Gegen die ungeprüfte Übernahme der Anforderungen für elektronische Vertrauensdienste in den Telekommunikationsbereich, wie sie von der EU vorgegeben worden sind, bestehen seitens der Telekommunikationsbranche daher nur insoweit Bedenken, als an die Identifikation von Mobilfunkkunden nicht per se die gleich hohen Anforderungen wie an Vertrauensdienste generell gestellt werden können.

Das ergibt sich bereits aus dem Grundsatz der Verhältnismäßigkeit: Die Registrierung des Telekommunikationskunden ist nur ein Element eines großen Portfolios an ermittlungsunterstützenden Maßnahmen, die Behörden im Bereich der Telekommunikation zur Verfügung stehen. Selbst bei nicht registrierten SIM-Karten stehen den Ermittlungsbehörden noch sämtliche anderen Methoden der legal Interception zur Verfügung, die es ermöglichen, einem Täter, der einen Mobilfunkanschluss nutzt, habhaft zu werden. Daneben ist auch hier wieder das Argument aufzuführen, dass es Tätern leichtfällt, sich auf alternativen Wegen „anonyme“ SIM-Karten zu besorgen.

Ein Online- identifikationsverfahren dürfte daher zum überwiegenden Teil (wie auch Erfahrungen in der Schweiz gezeigt haben) von lauteren Nutzern angewendet werden.

Letztlich sind auch die mit einem elektronischen Vertrauensdienst verbundenen Gefahren kriminalistischer wie wirtschaftlicher Art in keiner Weise mit den Risiken eines unrechtmäßig registrierten Mobilfunkanschlusses zu vergleichen. Weder dient ein Mobilfunkanschluss weiteren Identifikationszwecken z.B. im Rahmen der Ausstellung einer digitalen Signatur, noch sind die wirtschaftlichen Risiken, die bei Nutzung eines Mobilfunkanschlusses entstehen können, mit denen des z.B. Abschlusses eines Bankkontos o.ä. zu vergleichen.

Es sollte daher ein schlanker, für den Kunden einfach und schnell zu handhabender Prozess bevorzugt werden, der die oben dargestellten Sicherheitskriterien erfüllt und damit bereits über die Fähigkeiten eines Call-Shop Betreibers, mit dem und dessen Kenntnissen an Sicherheitsmaßnahmen das Verfahren zu vergleichen ist, weit hinausgeht.

Als Beispiel können hier die Sicherheitsanforderungen der Kommission für Jugendmedienschutz (KJM) bei der Identifizierung von Teilnehmern an geschlossenen Benutzergruppen für jugendgefährdende Telemedieninhalte herangezogen werden. Die Risikobetrachtung dürfte hierbei sogar auf Grund des hohen Anspruchs des Jugendschutzes vor unangemessenen Inhalten oder der nicht für Minderjährige zulässigen Teilnahme an Glücksspielen noch höher ausfallen als bei der Registrierung von SIM-Karten. Dennoch sind nach dem Prüfraster der KJM Verfahren, wie das nachfolgend beschriebene Autoident-Verfahren, als geeignet angesehen worden, um gem. dem Jugendmedienschutz-Staatsvertrag eine Volljährigkeitsprüfung durchzuführen. Die KJM betrachtet dabei Verfahren als anwendbar, die geeignet sind, die Volljährigkeit mit hoher Wahrscheinlichkeit (Plausibilitätsprüfung) festzustellen. Ferner fordert die KJM eine Lebenderkennung und ausreichende Bildqualität bei der Prüfung der Person sowie die Inaugenscheinnahme des Ausweises von beiden Seiten. Laut KJM kann bei Prüfungen von eine face-to-face Kontrolle abgesehen werden, wenn die Identifizierung mittels einer Software durch einen Vergleich der biometrischen Daten des Ausweisdokuments und einem Lichtbild des zu identifizierenden sowie einer automatischen Erfassung der Daten des Ausweisdokumentes erfolgt.

c. *Wenn ein Einsatz erwogen wird, bitte stellen Sie das Verfahren samt Gefährdungspotential und entsprechend möglichen Sicherungsvorkehrungen/-maßnahmen dar.*

Aus Sicht der Branche müssen Vorgaben für die Zukunft technologie-offen ausgestaltet werden, da sich die technischen Möglichkeiten rapide weiter entwickeln. Somit darf nicht lediglich der heutige Stand zementiert werden.

Das beispielsweise in der Schweiz eingesetzte (und u.a. auch von der KJM als zulässig bewertete) Verfahren im Rahmen der Mobilfunkkundenidentifizierung sieht derzeit folgende Schritte vor, die ggf. durch einzelne interaktive Elemente ergänzt werden könnten:

1. Aufnahme beider Seiten des ID-Dokuments

2. Aufnahme eines Selfie Videos

3. Abgleich von Bild und Personendaten

4. Ausgabe eines Ergebnisses

Neben der Liveness detection werden auch im Rahmen der Prüfung der Dokumentendaten Plausibilitätstests bezüglich der in der Visuellen Zone (gemeint sind alle Klartextelemente auf dem Ausweis - VIZ) und der Machine Readable Zone (MRZ) enthaltenen Daten durchgeführt. Es werden ferner durch Einsatz von Techniken künstlicher Intelligenz die Sicherheitsmerkmale der Dokumente (z.B. Hologramme, Schriftarten, Kinematische Effekte) auf Authentizität überprüft, es können Prüfungen von Referenzdatenbanken sowohl in Bezug auf die Dokumenten- und Sicherheitsmerkmale als auch die Richtigkeit der enthaltenen Personendaten und Checksummenberechnungen durchgeführt werden. Die Sicherung der Aktualität der Aufnahmen ist ein wichtiger Faktor.

In Zweifelsfällen können vom System automatisch manuelle Nachkontrollen durch ein geführtes System angestoßen werden, die false acceptances praktisch vollständig ausschließen. Solche manuelle Nachkontrollen können das Vertrauen in die Verfahren weiter stärken, sollten jedoch auf Einzelfällt beschränkt bleiben.

Bei Bedarf/technischen Problemen sollten Kunden in einen herkömmlichen VideoIdent-Prozess überführt werden können. Alternativ wäre möglich, dass Agents die Daten bei Nicht-Lesbarkeit oder anderen Grenzfällen manuell prüfen können. Hier müsste auch gewährleistet bleiben, dass sich im Ablehnungsfall ein Kunde noch an einen menschlichen Support für eine Überprüfung dieser Entscheidung wenden kann.

3. Aktualität bei Vorabverifikation:

Grundsätzliche Vorbemerkung zur Verfahrensbeschreibung nach Ziffer 3 der aktuellen Verfügung:

Geldwäscherechtlich verpflichtete Unternehmen (bspw. Banken) sind ebenfalls zur Identifizierung ihrer Kunden verpflichtet. Hinsichtlich des Inhalts der einzuholenden Informationen, der Unterlagen anhand derer eine Identitätsprüfung zu erfolgen hat, der erforderlichen Speicherung sowie der Anforderungen, die an die konkreten Identifizierungsverfahren gestellt werden, gibt es zwischen GwG und TKG zahlreiche Überschneidungen. Teilweise gehen die Anforderungen nach GwG allerdings über die Anforderungen nach TKG hinaus. Daneben sind geldwäscherechtlich verpflichtete Unternehmen verpflichtet, die Identitätsdaten des jeweiligen Kunden in angemessenem zeitlichem Abstand sowie anlassbezogen zu aktualisieren. Die Deutsche Kreditwirtschaft hat ggü. dem BMWi bereits das Interesse und die Bereitschaft bekundet, ihren Kunden die Möglichkeit zur Nutzung ihrer bei den Banken vorliegenden Identitätsdaten zur Vorabverifikation im TKG-Kontext über das Online-Banking anzubieten. Diese Form der Nachnutzung von vorab verifizierten Identitätsdaten wird durch die Formulierung unter Ziffer 3 der aktuellen Verfügung, dass die Daten „... bei einem eigens mit einer Identitätsprüfung beauftragten Dritten zum Zwecke des Abrufes vorgehalten werden“ gegenwärtig verhindert. Da diese Formulierung nach unserer Einschätzung eher erläuternden (dadurch aber nicht nachvollziehbar einschränkenden) Charakter hat, sollte sie gestrichen werden. Vielmehr sollten Identifizierungsdaten, die nach den Vorgaben des zum Teil strengeren GwGs gesetzeskonform im GwG-Kontext weiterverwendet werden können auch – neben klassischen AutoIdent-verfahren - für eine Vorabverifikation im TKG-Kontext herangezogen werden können.

a. *Wie wird bei Vorabverifikationsverfahren im Sinne von Verfahren unter Ziffer 3 der Verfügung sichergestellt, dass dem mit der Identitätsprüfung beauftragten Dritten auch Aktualisierungen, zum Beispiel von Adressdaten im Falle eines Umzugs / Ummeldung des Kunden, zur Kenntnis gelangen?*

Grundsätzlich obliegt dem Anbieter eines Vorabverifikationsverfahrens i.S.v. Verfahren unter Ziffer 3 der Verfügung die ausreichende Sicherstellung, dass dem Anbieter von Telekommunikationsdiensten nur aktuelle bzw. sachlich richtige Kundendaten übermittelt werden. Die Prüfung von Adressen auf Richtigkeit, Plausibilität und Aktualität können bspw. über Fuzzy Logic Prozesse, z.B. unter Zuhilfenahme von Datenbanken der Deutschen Post durchgeführt werden. Fällt eine Fuzzy-Prüfung negativ aus, kann auf die menschliche Nachkontrolle verwiesen werden.

b. *Gibt es in Ansehung des zeitlichen Auseinanderfallens von Verifikationszeitpunkt und dem Abruf der Daten durch den Diensteanbieter beispielsweise regelmäßige Aktualisierungsabfragen oder hat die Vorabverifikation nur eine befristete Wirkung?*

Die Zeiträume zwischen Vorabidentifikation und Datenabruf können flexibel angepasst werden. Solange nicht durch entsprechende Zeitstempel und Metadaten der Zusammenhang beider Aktionen sichergestellt werden kann, kann der Nutzer zur erneuten Durchführung der Identifikation aufgefordert werden. Die Aufforderung könnte im Rahmen der rechtlichen Möglichkeiten durch die Telekommunikationsanbieter erfolgen.

Geldwäscherechtlich verpflichtete Unternehmen sind gesetzlich verpflichtet, die Identitätsdaten ihrer Kunden in der laufenden Geschäftsbeziehung aktuell zu halten Identifizierungsdaten, die im GwG-Kontext gesetzeskonform weiterverwendet werden können, sollten daher – im Auftrag und mit Zustimmung des Nutzers – auch für die Identifizierung nach §111 TKG genutzt werden können. Da die Identitätsdaten bereits vorab von einem regulierten Unternehmen geprüft wurden, ist eine nochmalige Überprüfung der Korrektheit durch den Mobilfunkprovider bei Nachnutzung von GWG-geprüften Daten nicht notwendig.

c. *Sofern derartige Sicherstellungsmaßnahmen bislang nicht praktiziert werden, bestehen Bedenken gegen die Einführung von derartigen Maßnahmen?*

In jedem Fall müssten etwaige Vorgaben für Aktualisierungsabfragen die datenschutzrechtlichen Bestimmungen berücksichtigen bzw. hierzu klare Berechtigungen beinhalten.

Geldwäscherechtlich verpflichtete Unternehmen sind ohnehin zur fortlaufenden und anlassbezogenen Aktualisierung von Identifizierungsdaten verpflichtet. Durch die gesetzliche Verpflichtung nach GWG besteht auch die datenschutzrechtliche Zulässigkeit zur Aktualisierung und Speicherung dieser Daten.

4. *Juristische Personen und Personengesellschaften*

a. *Wie relevant ist die Nutzung von Prepaid SIM-Karten durch juristische Personen und Personengesellschaften?*

Die Relevanz der Nutzung von Prepaid SIM-Karten durch juristische Personen und Personengesellschaften ist in der Praxis eher gering. Allerdings stellen wir in letzter Zeit aufgrund von Prepaid-IoT-Angeboten ein signifikant steigendes Interesse von Unternehmenskunden an solchen Produkten und damit einhergehend auch eine steigende Anzahl von Vertragsabschlüssen fest. Das Kernproblem ist hier die Überprüfung der Zeichnungs- bzw. Vertretungsberechtigung von handelnden natürlichen Personen für das Unternehmen. Von IoT-Anbindungen geht kein Gefährdungspotenzial im Hinblick auf die anonyme interpersonelle Kommunikation aus.

b. Besteht hier ein Bedarf zur Einführung eines spezifischen vereinfachten Identifizierungsverfahrens?

Ein neues spezifisches vereinfachtes Identifizierungsverfahrens für juristische Personen ist im Prepaid-Bereich kein drängendes Thema. Aus Branchensicht ist die Möglichkeit einer Prüfung anhand der „Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten“, wie in § 111 Abs. 1 S. 3 Nr. 7 TKG vorgesehen, ausreichend.

Die Durchführung eines Autoident-Verfahrens ist unter Einbindung von Firmendatenbanken mit Zugriff aus Handelsregisterdaten grundsätzlich möglich.

c. Bestehen Bedenken gegen z. B. eine E-Mail-Übersendung von digitalen Kopien von Registerauszügen im Sinne des § 111 Absatz 1 Satz 3 Nr. 7 TKG?

Da Handelsregister grundsätzlich öffentlich sind, bestehen hier per se keine Bedenken. Eine Übermittlung per E-Mail sollte jedoch bei Einsatz von Datenbankabfragen und elektronischer Dokumentenerfassung entbehrlich sein. Je nach Geschäftsfall ist es jedoch geboten risikoorientiert ergänzende Nachweise zu prüfen. Erfahrungen aus dem Postpay-Segment zeigen, dass derzeit Registerauszüge häufig manipuliert werden, so dass unter Nutzung gefälschter Ausweise ein Vertragsabschluss durchgeführt wird. Es gibt alternativ kundenfreundliche Methoden, die dazu noch eine höhere Sicherheit bieten. Beispielsweise die maschinelle Abfrage des Handelsregisterauszugs. Trotz der Kosten, die ein solcher Abzug verursacht, ist der Einsatz gegenüber der Einreichung einer digitalen Kopie vermutlich kostenneutral, da zwar hier nicht die Abfragekosten, aber dafür nachgelagerte Prüfkosten entstehen würden.

Gegen die E-Mail-Übersendung würden zudem Bedenken bestehen, wenn keine ausreichende Verschlüsselung erfolgt. Bekanntlich sind E-Mails sonst nicht ausreichend gegen Einsichtnahme geschützt, die enthaltenen Informationen sind vertraulich, da sie eine Geschäftsbeziehung betreffen. Als Alternative könnte ggf. ein (ausreichend verschlüsseltes) Uploadportal in Erwägung gezogen werden.

5. Barrierefreiheit

a. Wie wird in der aktuellen Praxis der Identifizierungsverfahren seitens der Telekommunikationsdiensteanbieter auf die Bedürfnisse von Menschen mit Behinderungen eingegangen?

Für Telekommunikationsdiensteanbieter besteht, sofern die Angebote von Verifizierungsanbietern die Bedürfnisse von Menschen mit Behinderung im Einzelfall nicht ausreichend gerecht werden, insbesondere die Möglichkeit der Datenlegitimierung beim Händler.

Verfahren 1 „Post-Ident“: Gem. Verfügung ist die Vertretung durch einen Betreuer für Prepaid nicht gestattet, sofern die Anwesenheit des Ausweisinhaber nicht möglich ist.

Verfahren 2 „Videoident“: Hier ist die Identitätsprüfung aus unserer Sicht unter zusätzlicher Anwesenheit des Betreuers oder Dolmetschers von der Verfügung umfasst.

Verfahren 3 „Vertrauensdiensteanbieter & Bestandskunden“ derzeit kein sinnvoller Einsatz möglich, da der Wortlaut der Verfügung quasi den Aufwand einer Erstidentitätsprüfung erzeugt.

Verfahren 4 „eID online“ ist aus unserer Sicht barrierefrei umsetzbar.

b. *Gibt es Vorschläge für eine Anpassung der Vorgaben für Identifizierungsverfahren, um diese an die Bedürfnisse von Menschen mit Behinderungen anzupassen und barrierefreier zu gestalten?*

Grundsätzlich ist das Autoident-Verfahren gleichermaßen von Menschen mit Behinderungen anwendbar, wie das Videoident-Verfahren. Allenfalls bei Sehbehinderten dürften Schwierigkeiten bestehen.

Insgesamt wird eine detailreiche Beschreibung bis auf die Ebene unternehmensinterner einzelner Prozessschritte zwangsläufig dazu führen, dass sowohl ungewollte Barrieren als auch weiße Flecken und Redundanzen entstehen. Insofern sind die Ausgrenzungen von ganzen ethnischen Gruppen, oder Personen mit Behinderungen, bereits in der heutigen Verfügung angelegt.

Bei Menschen mit Sprach- und Hörbehinderungen dürfte das Autoident-Verfahren deutliche Vorteile bieten, da es sowohl Hemmschwellen bei der Artikulation vermeidet als auch weitestgehend mit einer schriftlichen Interaktion auskommt. Für Sehbehinderte käme in Betracht, entweder die NFC Funktion einzubinden, die das Präsentieren des Ausweises in eine Kamera vermeidet. Ggf. könnte die Aufnahme des Selfievideos durch akustische Signale erleichtert werden.

Gegenwärtig sind leider keine Verfahren verfügbar, um Menschen, die von der Ausweispflicht befreit sind, zu legitimieren. Sollte auch weiterhin das Kontrollmaß und nicht das Kontrollziel definiert werden, wäre eine Ergänzung erforderlich. Die Verfügung sieht an verschiedenen Stellen ein Gespräch vor, was aus Gründen der Barrierefreiheit und Rechtssicherheit auch Betreuer-/Dolmetscher-leistungen, oder auch einen Chat als legitimiertes Vorgehen einbeziehen sollte.

c. *Würden entsprechende Anpassungen zusätzliche Sicherheitsrisiken mit sich bringen und wie könnte man diesen begegnen?*

Erhöhte Sicherheitsrisiken bei Menschen mit Behinderungen sind nicht erkennbar.