bitkom

Stellungnahme

Mai 2024

Referentenentwurf Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung

Zusammenfassung

Bitkom begrüßt den Referentenentwurf zur Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung. Die Angleichung der Identifizierungsverfahren eID, Video- und Autoident ist ein wichtiger Schritt in der Digitalisierung von Prozessen im Finanzbereich. Gleichzeitig wird die Verpflichtung zur Einführung von eID-Verfahren zu einer Verbreitung dieses Verfahrens in der Bevölkerung führen und schafft damit einen wichtigen Anwendungsfall. Damit passen wir uns auch den europäischen Standards an. Solange die Verbreitung des deutschen eID-Verfahrens allerdings abhängig ist von externen Faktoren wie des derzeit analogen eID-Rücksetzungsdienstes, werden alternative Verfahren weiter benötigt. Die Möglichkeit des Einsatzes teil- und voll-automatisierter Verfahren ist daher aus unserer Sicht sehr zu begrüßen. Durch diese Verfahren können Identitätsprüfungen zukünftig voraussichtlich kostengünstiger durchgeführt werden.

Gedanklich geht der Referentenentwurf in eine gute Richtung – technisch und sprachlich gibt es jedoch Verbesserungsbedarf.

Videoidentifizierung

Die Begriffe „gleichwertige Art und Weise“ sollten konkretisiert werden, wenn es darum geht, Identifizierungsverfahren zur Verfügung stellen zu müssen. Dies gilt insbesondere im Umgang mit ausländischen Ausweisdokumenten. Da ein nicht unerheblicher Teil des Traffics bei deutschen Identanbietern aus dem europäischen und außereuropäischen Ausland kommt, empfehlen wir dringend, die Vorgehensweise bei Bürgern aus Ländern zu konkretisieren, die kein deutsches oder europäisches eID-Verfahren nutzen können. Diese müssten dann nicht zwingend auch die deutsche eID als Verfahren angeboten bekommen. Als Alternative sollten Anbieter auch europäische eID-Verfahren anbieten dürfen.

Die in §12 Abs. 3 aufgeführten Schulungen der Mitarbeiter sollten a) regelmäßig stattfinden, b) durch jeden beteiligten MA dokumentiert werden und c) im Fehlerfall ad hoc erfolgen. Bitkom empfiehlt außerdem eine Zertifizierung nach ETSI TS 119 461 des gesamten Schulungskonzepts inklusive regelmäßiger Auditierung durch eine Konformitätsbewertungsstelle.

Das „ausdrückliche Einverständnis", welches eine Person zu Beginn des Verfahrens zur Identifizierung geben muss, sollte klarer definiert werden. Hier stellt sich die Frage, ob eine mündliche Zustimmung ausreicht oder bspw. ein Haken gesetzt werden muss, bevor ein Gespräch mit dem Agent geführt wird.

Prüfung von Sicherheitsmerkmalen

Der **Prüfung von Sicherheitsmerkmalen** (§11) wird gemäß dem vorliegenden Entwurf, richtigerweise, eine hohe Bedeutung beigemessen. Hierbei werden die zu prüfenden Kategorien reduziert und die Merkmale konkretisiert. In ihrer derzeitigen Fassung stellen die Änderungen der zu prüfenden Sicherheitsmerkmale ein de facto Verbot des Videoident-Verfahrens dar. Das gilt insbesondere auch für Ausweisdokumente aus bestimmten EU-Mitgliedstaaten, so dass die Vorgaben dazu führen würden, dass natürliche Personen aus EU-Mitgliedstaaten nicht mehr unter Nutzung des Videoidentifizierungsverfahrens identifiziert werden könnten. Es bestehen erhebliche Zweifel, ob dieser indirekte Ausschluss mit dem europäischen Recht vereinbar ist.

Im Vergleich zum BaFin-Rundschreiben 3/2017 wurden in §11 im Referentenentwurf die Sicherheitsmerkmale „Zero-Order-Device", „taktile Bereiche", „Prägung" neu eingeführt. Dabei lassen sich zumindest haptische Sicherheitsmerkmale wie „taktile Bereiche" und eine „Prägung" online nicht über ein Videoident-Verfahren prüfen, wie auch das BSI im Anforderungskatalog zur Prüfung von Identifikationsverfahren gemäß TR-03147 in Version 1.0.6 anmerkt. Aus diesem Grund sollten diese Merkmale nicht in den Katalog zur zwingenden Prüfung aufgenommen werden.

Des Weiteren wird in §11 Abs. 2 gefordert, dass alle Individualdaten in Sicherheitsmerkmalen zu prüfen sind. Es ist praktisch nicht möglich, alle in der neuen Verordnung aufgeführten Individualdaten in Sicherheitsmerkmalen im Videoident-Verfahren zu prüfen, da auf vielen Ausweisdokumenten eine sehr hohe Anzahl an individualisierten Merkmalen vorhanden ist die z.T. sehr klein sind und nur mit unverhältnismäßig hohem Aufwand geprüft werden können. Wir empfehlen diesen Passus ersatzlos zu streichen, da er in der Realität nicht umsetzbar erscheint.

Stand jetzt wäre ein neuer deutscher Personalausweis so nicht prüfbar; während er reichlich beugungsoptische Merkmale besitzt und man aus den Personalisierungstechniken das Laserkippbild verifizieren kann, besitzt der deutsche Personalausweis kein transparentes Sichtfenster und wäre somit nicht nutzbar für die Videoidentifizierung. **Zusammengefasst plädieren wir daher stark dafür, die alten technischen Anforderungen an die Identifizierung von Ausweisdokumenten per Videoident aus dem BaFin Rundschreiben 03/2017 beizubehalten.**

Mehr Sicherheit durch NFC

Im Rahmen der Prüfung von Sicherheitsmerkmalen möchten wir das Auslesen von Chip gebundenen Daten aus qualifizierten, digital signierten Ausweisdokumenten nach dem globalen ICAO-Standard in die Diskussion einbringen. Bei Dokumenten, bei denen ein qualifiziertes Auslesen möglich ist, sollte dies ein zwingend zu prüfendes Sicherheitsmerkmal sein. In diesem Kontext könnten Sicherheitskonfidenzprüfungen im Rahmen von §11 entfallen, die die Authentizität der Daten gewährleistet hätten, die aus dem Chip ausgelesen wurden. In der Kombination mit der automatisierten Video-Ident Prüfung, wird ein nutzerfreundliches und sichereres Verfahren erreicht. Zudem ist die ICAO-konforme eMRTD- (electronic Machine Readable Travel Document) Funktion automatisch im Ausweisdokument freigeschaltet, weshalb bereits heute hunderte Millionen EU-Bürger mit diesem Verfahren erreicht werden können.

Abbruch des Verfahrens

Bei einem Abbruch des Verfahrens sollte eine Wiederholung der Videoidentifizierung möglich sein, sofern kein Betrugsverdacht besteht. Damit würde die Möglichkeit eingeräumt, z.B. unzureichende Lichtverhältnisse zu beheben. Diese Möglichkeit besteht bereits im TKG. Die Qualität der Übertragung ist anhand ETSI TS 119 461 zu bemessen.

Technische Anforderungen

In §9 (4) als auch in §13 werden **Anforderungen an die Bildauflösung und die Reaktionsgeschwindigkeit** der Nutzer gestellt, die aus unserer Sicht zwar wünschenswert, aber aktuell noch realitätsfern sind. Zum einen verfügen zahlreiche Nutzer nicht über Endgeräte mit einer entsprechenden Auflösung (insbesondere bei der nutzerseitigen Kamera), um dieser Anforderung gerecht werden zu können. Zum anderen setzt die Regelung voraus, dass clientseitig netzwerktechnisch keine Restriktionen vorliegen, die Bürger mit älteren Geräten oder geringerem Datenvolumen von der Nutzung des Videoidentifikationsservices ausschließen. Hinzu kommt eine in §13 Abs. 1 vorausgesetzte, sehr schnell angesetzte Reaktionszeit der Nutzer von unter einer Sekunde, wodurch zum Beispiel ältere Personen oder Personen mit Einschränkungen benachteiligt werden. Derart detaillierte technische Anforderungen erreichen lediglich eine Einschränkung der Nutzung von Fernidentifikationsverfahren und sollten daher gestrichen oder lediglich Empfehlungen formuliert werden.

Räumlichkeiten

Der Begriff der „Zugangskontrolle“ wie verwendet in §7 muss definiert werden. Wir regen außerdem an, zur weiteren Spezifizierung der Anforderungen an die Räumlichkeiten auf ETSI EN 319 401 zu verweisen.

Übermittlung einer Ziffernfolge

Die Übermittlung der Ziffernfolge sollte durch geeignete Maßnahmen substituierbar sein. Hierfür ist zu definieren, welcher Schutzmechanismus mit der Ziffernfolge erreicht werden soll. Soll bspw. die Wiederholbarkeit durch einen Angreifer erschwert werden, wäre die Übermittlung einer Ziffernfolge an eine E-Mailadresse keine geeignete Maßnahme, ein Device-Fingerprint aber schon. Daher sollte die Formulierung im Entwurf „...insbesondere per E-Mail oder per SMS“ klarstellend auch die Nutzung weiterer technischer Möglichkeiten zur TAN-Übermittlung wie z.B. eine Push-Notification zulassen. Außerdem sollte die Möglichkeit bestehen, das One Time Password in einem Videoidentifizierungsverfahren dem Agenten mündlich zu übermitteln.

Teilautomatisierte Verfahren

Die ausdrückliche Zulassung von **Teilautomatisierung** in Teilschritten ist eine wesentliche Verbesserung zum aktuellen Prozess. Das Zusammenspiel von automatisierten, KI-basierten Schritten sowie einer direkten oder indirekten menschlichen Prüfung kann den Schutz vor Missbrauch wie Identitätsdiebstahl erhöhen. Dennoch bietet der vorliegende Referentenentwurf Raum für Verbesserung und Präzision einzelner Formulierungen.

Die in §9 Abs. 2 geforderte **"Videoidentifizierung in Echtzeit und ohne Unterbrechung"** erfordert eine Klarstellung, ob die aufgezeichnete Prüfung der Teilprozessschritte (§9 Absatz 5 und §§ 11 und 12) in einem unterbrechungsfreien Stream mit den synchronen Nutzer-Mitarbeiter-Prozessschritten (§§ 14 u. 15) aufgezeichnet werden muss oder ob die Aufzeichnung der Teilschritte auch in mehreren, von der Aufzeichnung des Nutzer-Mitarbeiter-Videomitschnittes getrennten, Sequenzen zulässig ist. Im Zweifel sollten beide Varianten zulässig sein.

Definition der Teilautomatisierung

Zudem gilt es konkreter zu erläutern, wie Teilautomatisierung zu definieren ist. Insbesondere die Frage, ob ein solches Verfahren eine kurze Interaktion zwischen Kunden und Agenten beinhaltet oder ob manuelle Checks durch Personen während des, bzw. nach dem Identifizierungsprozess vorgenommen werden, muss dringend beantwortet werden.

Social Engineering

"**Social Engineering**" ist bereits heute das am häufigsten festgestellte Betrugsszenario bei GwG-Verpflichteten im Bereich der Fernidentifizierung. Bitkom weist darauf hin, dass Social Engineering ein erhöhtes Gefahrenpotenzial für alle Identifizierungsverfahren birgt. Dieses gilt es zu beachten, wenn neue Verfahren im geldwäscherechtlichen Bereich zur Identifizierung von Personen eingeführt werden. Es ist daher zu empfehlen, die Auswirkungen von Social Engineering in den einzelnen

Verfahren zu bewerten und mit Gegenmaßnahmen eine ausreichende Sicherheit zu gewährleisten.

Prüfverfahren und Zulassung

Es sollte klargestellt werden, nach welchem Standard, bzw. welcher Governance das **Prüfverfahren** durchgeführt und damit die Verfahren zertifiziert werden. Es ist wünschenswert, die angewandten Prüfverfahren frühzeitig zu konkretisieren. So könnten sich die Prüfkriterien an bestehenden Technischen Richtlinien, wie etwa der TR-03107 oder TR-03147 orientieren. In der jetzigen Fassung des Entwurfs sehen wir ein weiteres Problem in der fehlenden Definition der Gleichwertigkeit der einzelnen Verfahren. Abhilfe würde eine Zertifizierung nach ETSI schaffen, die ein eIDAS-Vertrauensniveau für diese Verfahren festlegt, z.B. substantial.

Die Vorgabe für eine Erprobung gem. § 17 Abs. 2 Nr. 2 GwVideoIdentV dürfte in der Praxis kaum umsetzbar sein. Die Risikoklassifizierung eines Kunden erfolgt in der Regel erst nach Abschluss der Identifizierung und der Erfüllung der allgemeinen Sorgfaltspflichten nach § 10 Abs. 1 GwG. Erst dann liegen dem Verpflichteten genügend Informationen vor, um überhaupt bewerten zu können, ob im Hinblick auf die zu identifizierende Person bzw. auf die jeweilige Geschäftsbeziehung, Hinweise auf ein höheres Risiko der Geldwäsche oder Terrorismusfinanzierung vorliegen.

Ebenso müssen die „Anhaltspunkte“ die zu einem Verbot des Verfahrens nach § 17 Abs. 3 führen können klar definiert werden, um eine subjektive Bewertung zu verhindern. Außerdem sollte die Möglichkeit, die Weiterverwendung des Verfahrens zu verbieten, auf die Erprobungsphase beschränkt werden.

Die Erprobung sollte außerdem nicht nur durch Verpflichtete nach § 2 Abs. 1 Satz 1 GwG (Kreditinstitute iSd § 1 Abs. 1 KWG) erfolgen. Eine Erweiterung (zumindest) in Bezug auf alle Verpflichtete iSd § 2 GwG aus dem Finanzsektor und auf die Hersteller der Verfahren (unabhängig von deren Beauftragung durch einen Verpflichteten) wäre empfehlenswert.

Sonstiges

Um zu vermeiden, dass die Analyse und damit die Auslegung der Zulässigkeit bestimmter Ausweisdokumente den einzelnen Anbietern überlassen wird (was zu Auslegungsasymmetrien und daher zur Unsicherheit führen könnte), wäre es wünschenswert, § 10 durch eine **detaillierte Liste zulässiger Ausweisdokumente** zu ergänzen. Zwingend aufgenommen werden sollten ePerso, eAT oder ePass + Meldebescheinigung oder ein anerkanntes Ausweisdokument eines anderen Landes.

Die Aufbewahrung- und Aufzeichnungspflicht in §18 muss sowohl für das Video-Ident, als auch das teilautomatisierte Verfahren gelten. Zudem sollte in § 18 Abs. 3 GwVideoIdentV klargestellt werden, dass analog § 8 Abs. 2 GwVideoIdentV für die Aufzeichnung und Aufbewahrung § 8 GwG entsprechend gilt.

Zudem bedarf es aufgrund der Vorgaben des § 5 Abs. 2 GwVideoIdentV, wonach das (teilautomatisierte) Videoidentifizierungsverfahren nur verwendet werden darf, wenn

in gleichwertiger Art und Weise auch ein eID-Verfahren angeboten wird, einer längeren Übergangsfrist als nach § 21 Abs. 1 GwVideoIdentV vorgesehen. Insbesondere Verpflichtete, die aktuell nur das Videoidentifizierungsverfahren anbieten, werden voraussichtlich mehr Zeit benötigen, um sämtliche Produktstrecken an die Anforderungen des § 5 Abs. 2 GwVideoIdentV in technischer Hinsicht anzupassen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Clemens Schleupner | Referent Vertrauensdienste & Digitale Identitäten
T 030 27576-424 | c.schleupner@bitkom.org

Lukas Marschallek | Referent Digital Banking & Financial Services
T 030 27576-551 | l.marschallek@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digitale Identitäten
AK Anwendung elektronischer Vertrauensdienste
AK FinTechs & Digital Banking