

Stellungnahme WebID Solutions GmbH zum Referentenentwurf des Bundesministeriums der Finanzen: Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung

Hamburg, 07.05.2024

Die WebID Solutions GmbH begrüßt den Entwurf ausdrücklich und möchte im Folgenden auf einzelne geldwäsche-rechtlich relevante Faktoren hinweisen, die für einen nachhaltigen und langfristig sicheren Betrieb von Videoidentifizierungsverfahren unerlässlich sind. Das Unternehmen ist mit über 20 Mio. durchgeführten, GwG-konformen Videoidentifizierungen in den vergangenen 11 Jahren einer der Marktführer. Im Rahmen dieser über einer Dekade gesammelten Erfahrungen im Kontext der IT- und Betrugssicherheit des Verfahrens führen wir im die folgenden Ergänzungen bzw. Änderungsvorschläge aus:

eID - § 5 GwVideoidentV

WebID unterstützt die in § 5 vorgesehene breite Etablierung der eID in Deutschland und bietet vielen Kunden bereits heute eine Auswahl unterschiedlicher Identifizierungsmöglichkeiten, u.a. mit der eID. Vor diesem Hintergrund möchte das Unternehmen noch einmal betonen, dass insbesondere die Wahlmöglichkeit der Identifizierungsmethode essenziell für hohe Nutzungsquoten ist.

Schulungsqualität - §6 GwVideoidentV

Den in § 6 des Entwurfs genannten Anforderungen stimmen wir vollends zu. Für eine adäquate Sicherheit reicht es aus der Perspektive der WebID jedoch nicht aus, die Schulung der Mitarbeiter vorzuschreiben. WebID empfiehlt eine Zertifizierung des gesamten Schulungskonzeptes inklusive regelmäßiger Auditierung durch eine Konformitätsbewertungsstelle. Hier kann auf bereits etablierte Prüfmechanismen aus der eIDAS aufgebaut werden. Hierbei ist insbesondere die Sprachkenntnis der jeweiligen Mitarbeiter zu prüfen, da das Aufdecken von "Social Engineering" und "Friendly Fraud" nur mit umfassenden Sprachkenntnissen möglich ist. Ebenfalls bedarf es durch den Umgang mit besonders schutzwürdigen personenbezogenen Daten Sicherheitsüberprüfungen der jeweiligen Mitarbeiter.

Deshalb schlägt WebID vor, durch Konformitätsbewertungsstellen zu bestätigende Schulungskonzepte und Personalüberprüfungen vorzusehen.

WebID unterstützt hierbei gerne bei der Entwicklung von eIDAS konformen standardisierten Schulungskonzepten und kann insb. durch WebIDs Fraud Analysis Team Praxiswissen einbringen, um Prozesse noch sicherer zu gestalten. Gerne können wir dafür auch unser Schulungskonzept zur Verfügung stellen.

Anforderungen an die Überprüfung von Dokumenten - §10 und §11 GwVideoidentV

Die in § 10 Abs. 2 und § 11 Abs. 4 (im Vergleich zum BaFin RS 2017) vorgesehene Verschärfung der Anforderungen würde aus der Perspektive WebIDs dazu führen, dass nur eine sehr geringe Anzahl von Ausweisdokumenten im Zuge einer Videoidentifikation überprüft werden könnte.

So wäre beispielsweise eine Identifikation des deutschen Personalausweises, in einem Videoidentifizierungsverfahren in dieser Form nicht möglich: Die Kategorie 3 „Material“ in

§11 Abs. 4 enthält lediglich zwei Prüfmöglichkeiten. „Prägung“ und „Transparentes Fenster“. Da sich die Prägung in einem Videoanruf nicht überprüfen lässt und der deutsche Personalausweis kein transparentes Fenster besitzt – aus jeder Kategorie jedoch ein Merkmal überprüft werden muss, ist der deutsche „nPA“ nicht identifizierbar. Weiter ist die Überprüfung der Behördenkennziffer in dieser Form nicht möglich, da es zum aktuellen Zeitpunkt für Anbieter keine solche zu überprüfende Liste gibt.

WebID schlägt deshalb vor, die aus dem BaFin RS 2017 enthaltenen Sicherheitsmerkmale, Kategorien und Prozesse beizubehalten, da sich diese in den vergangenen 7 Jahren als sehr resilient ggü. Betrugsversuchen bewiesen haben.

Die Unmöglichkeit gilt hier gleichermaßen für das Videoidentverfahren sowie teilautomatisierte Verfahren. Weiter würde eine solche Komplikation des Verfahrens zu einer deutlichen Verteuerung und dem Ausschluss des Großteils aller Ausweisdokumente führen.

Social Engineering im Rahmen der Teilautomatisierung - §12 GwVideoidentV

WebID unterstützt grundsätzlich die im Referentenentwurf vorgesehene Teilautomatisierung (automatisierte Aufnahme eines Videos mit anschließender Überprüfung durch einen geschulten Agenten) insbesondere im Hinblick auf die Identifizierung von Ausweisdokumenten sowie biometrische Abgleiche mit Nachdruck. Diese ermöglicht eine gleichwertige Sicherheit bei niedrigeren Kosten.

WebID sieht jedoch die in § 12 Absatz 2 und 3 GwG vorgesehene tiefenpsychologische Überprüfung lediglich auf Basis von Videoaufnahmen – also ohne eine Interaktion zwischen dem Agenten und der zu identifizierenden Person) als kritisch. "Social Engineering" ist bereits heute das häufigste von WebID festgestellte Betrugsszenario bei GwG-Verpflichteten im Bereich der Fernidentifizierung. Zur Erkennung sowie zur Überprüfung einer freien Willensbekundung ist aus WebIDs Perspektive das situationsangepasste Nachfragen unerlässlich, welches zum jetzigen Zeitpunkt auch mit KI-Tools nicht abzubilden ist.

Wir empfehlen zur Vermeidung von "Social Engineering" und weiteren Betrugsszenarien ein teilautomatisiertes Identifizierungsverfahren um einen stark verkürzten (ca. 45 Sekunden) Video Call mit einem Agenten zu ergänzen, in dem der Agent die zu identifizierende Person nach dem Grund der Identifizierung fragt und so sich einen Eindruck verschaffen kann, ob möglicherweise ein Betrugsfall vorliegt.

Videoqualität - §9 §13

WebID unterstützt einheitliche Qualitätsanforderungen an die Bild- und Tonqualität, würde aber aufgrund der in Teilen schlechten Internetabdeckung in Deutschland, dazu raten, dass die Bildqualität während des Calls schwanken darf und nur im Rahmen der Ermittlung der Sicherheitsmerkmale den vorgegebenen Anforderungen konstant entsprechen muss.

Datenbank gestohlener Ausweisdokumente

Auch wenn dies im Referentenentwurf nicht erwähnt wird, möchte WebID dazu anregen, einen automatisierten Abgleich mit gestohlenen Ausweisdokumenten, ähnlich wie es bereits in Frankreich praktiziert wird, anzustreben. Dies kann als zusätzliche Sicherheitsebene bestimmte Betrugsszenarien verhindern.

Auslesen der CAN

Weiter möchte die WebID vorschlagen, dass es Identifizierungsdienstleister bei einer Fernidentifizierung ermöglicht wird, mit dem Auslesen der CAN die Echtheit des (deutschen) Ausweisdokumentes zu überprüfen. Aktuell nur für „Vor-Ort“ Szenarien vorgesehen, könnte damit eine zusätzliche Sicherheitsebene etabliert werden, welche insb. In Teil-Automatisierten Prozessen noch mehr Sicherheit schafft.

Vollautomatisierung §17 GwVideoidentV

WebID begrüßt grundsätzlich die Vollautomatisierung von Identifizierungsverfahren, wie bereits gemäß § 12 Absatz 1 Satz 2 und 3 GwG geregelt (anhand einer QES mit einer Referenzüberweisung oder durch die eID).

Weitere vollautomatisierte Identifizierungsverfahren haben aus WebIDs Perspektive beim aktuellen Stand der Technik jedoch zu viele Angriffsvektoren, in denen Sie keine gleichwertige Sicherheit bieten können. So können vollautomatisierte Verfahren Social Engineering zum aktuellen Zeitpunkt weder umfänglich erkennen, noch wäre eine solche Erkennung mit dem AI-Act konform.

Als Dienstleister für Finanzinstitute hat WebID seit geraumer Zeit vollautomatische Verfahren verschiedenster Art sowohl intern als auch extern getestet und erforscht. Zum aktuellen Zeitpunkt kann jedoch keines dieser vollautomatisierten Verfahren eine gleichwertige Sicherheit im Vergleich zur herkömmlichen Videoidentifizierung aufweisen. Vielmehr haben "Skandale" wie der CCC-Angriff und das daraufhin resultierende GEMATI-K-Verbot im Jahr 2022, sowie Berichte wie der von 404 Media aus diesem Jahr, insbesondere aber die rasanten Entwicklungen im Bereich Deepfakes, gezeigt, dass vollautomatisierte Verfahren ein Sicherheitsrisiko darstellen können. Sie bieten Angreifern die Möglichkeit, ihre Angriffe in kurzer Zeit enorm zu skalieren.

Diese Situation stellt insbesondere vor dem Hintergrund bereits verstärkter krimineller Geldwäsche-Strukturen in Deutschland ein erhebliches Risiko dar und könnte zu erheblichen Reputationsschäden führen, insbesondere vor dem Hintergrund der Wahl von Frankfurt als Standort für die AMLA.

Deshalb betrachtet WebID es als absolut entscheidend, dass die für diese Zwecke angekündigten Sicherheitsprüfungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Sicherheit attestieren, die der Videoidentifizierung gleichwertig ist und die gleichen Anforderungen wie das Videoident erfüllt. Diese Gleichwertigkeit muss durch umfangreiche Tests vor der Inbetriebnahme gegenüber dem BSI nachgewiesen werden.