Praktischer Angriff auf Video-Ident

Demonstration inhärenter Schwächen der videobasierten Echtheitsprüfung physischer ID-Dokumente

Martin Tschirsich
Chaos Computer Club
Version 1.2, 8. August 2022

Kurzfassung

Trotz nachgewiesener prinzipbedingter Sicherheitsmängel wird die videobasierte Online-Identifizierung, kurz Video-Ident, inzwischen regelmäßig zur Absicherung digitaler Unterschriften, elektronischer Patientenakten, von Sozialdaten und mehr eingesetzt. Dabei wird ein in die Kamera gehaltenes ID-Dokument mit der zu identifizierenden Person abgeglichen und im Videobild auf Echtheit geprüft. Der vorliegende Bericht beschreibt einen neuen Angriff auf das Verfahren mit und ohne menschlichen Operator, basierend auf videotechnischer Neukombination mehrerer Quell-Dokumente. Das Schadpotential wird praktisch demonstriert, indem unter falscher Identität auf elektronische Patientenakten zugegriffen sowie qualifizierte elektronische Signaturen erzeugt werden. Die Angriffe bleiben unerkannt. Die auch für Laien zugängliche Angriffstechnik bedarf geringer Vorbereitungszeit und bedingt keine relevanten Kosten. Vom weiteren Einsatz des Video-Idents wird abgeraten.

Inhalt

Einleitung

Seit den 1980er Jahren verdoppelt sich die weltweite Informationsspeicherkapazität etwa alle drei Jahre (Hilbert & López, 2011). Behörden, Banken, Versicherungen und Unternehmen verfügen über immer mehr personenbezogene Daten. Wer sich ausweisen kann, erlangt Zugriff und Rechte, diese entscheiden über gesellschaftliche Teilhabe und wirtschaftlichen Erfolg. Die Schadenshöhe im Fall eines Identitätsdiebstahls steigt damit stetig an. Mit einem immer höheren Sicherheitsniveau staatlich herausgegebener Identitäts-Nachweisdokumente (ID-Dokumente) wie dem Reisepass oder dem neuen Personalausweis wird daher versucht, dem ansonsten proportional steigenden Risiko für den Identitätsinhaber zu begegnen. So wurden zuletzt 2021 die optisch im Weiß- und UV-Licht sowie taktil überprüfbaren Sicherheitsmerkmale des Personalausweises „auf den neuesten Stand der Technik weiterentwickelt sowie um weitere, hochsichere Merkmale ergänzt“ (Bundesministerium des Innern, für Bau und Heimat, 2021). Auch dürfen Fotos für Personalausweise und Reisepässe künftig nur noch manipulationssicher aufgenommen werden, um sogenannte Morphing-Angriffe zu unterbinden. In Folge ist das Entdeckungsrisiko eines Angriffs auf die persönliche Identifizierung vor Ort, beispielsweise mittels manipulierter, voll-gefälschter oder gestohlener ID-Dokumente, sehr hoch. Zudem drohen schwere strafrechtliche Sanktionen.

Demgegenüber setzen Betreiber spätestens seit 2014 zunehmend auf das Video-Ident, eine Online-Identifizierung ohne persönliches Erscheinen vor Ort. Dabei wird das ID-Dokument zusammen mit der zu identifizierenden Person durch diese abgefilmt, das Video an den Video-Ident-Anbieter übertragen und von diesem im Videobild auf Echtheit geprüft. Das immer höhere Sicherheitsniveau staatlicher ID-Dokumente überträgt sich jedoch nicht auf das Videobild des ID-Dokuments. Es kommt im Gegenteil zu einer massiven Absenkung des Sicherheitsniveaus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seit 2017 wiederholt aufgezeigt, dass die Echtheitsprüfung der ID-Dokumente im Videobild mit einfachen Mitteln angreifbar ist (Bundesamt für Sicherheit in der Informationstechnik, 2018). Angriffe können weder verhindert noch erkannt werden. Das Entdeckungsrisiko eines Angriffs auf Video-Ident ist folglich gering. Strafrechtliche Sanktionen greifen mangels Rückverfolgbarkeit eines Online-Angriffs nicht. Wo ein höheres Entdeckungsrisiko „zu einem spürbaren Rückgang von Cyberkriminalität beitragen“ kann (Bundesministerium des Innern, für Bau und Heimat, 2021), führt ein geringeres Entdeckungsrisiko in diesem Fall zu dessen Anstieg. Belegen lässt sich das anhand der von den Video-Ident-Anbieter genannten hohen Betrugsraten von 5 % bis 10 % (Burt, 2022), mehrheitlich verursacht von Wiederholungstätern.

Bei Einsatz des Video-Idents trifft demnach ein wachsendes Schadpotential auf eine höhere Angriffswahrscheinlichkeit bei gesenktem Sicherheitsniveau, das Risiko steigt überproportional an. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) lehnt diese Identifizierungsmethode daher ab und hat zwischenzeitlich die datenschutzrechtliche Unzulässigkeit des Verfahrens „zum Schutz besonders schutzbedürftiger Kategorien von personenbezogenen Daten“ festgestellt (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 2021). In Deutschland betrifft dies beispielsweise den Zugriff auf die in Psychotherapie- und Arztpraxen, Krankenhäusern und bei Krankenkassen gespeicherten Gesundheitsdaten von 73 Millionen gesetzlich Krankenversicherten über die elektronische Patientenakte (ePA) nach § 341 SGB V. EU-weit sind rechtssichere digitale Unterschriften auf Grundlage qualifizierter Zertifikate (QES) betroffen, welche nach einem Video-Ident ausgestellt werden. Mit der kommenden eIDAS 2.0-Verordnung und der jüngst

verabschiedeten ETSI-Spezifikation TS 119 461 (ETSI, 2021) mit entsprechenden Regelungen für die videobasierte Fernidentifizierung ist mit einer weiteren Verschärfung dieses Problems zu rechnen.

Nachfolgend werden zunächst bekannte Angriffe und deren Auswirkung auf die weitere Verbreitung von Video-Ident und anschließend ein neuer, vereinfachter Angriff auf das Verfahren beschrieben, der mit reduziertem Aufwand auch gegen Video-Ident ohne menschlichen Operator zum Einsatz gebracht werden kann. Danach wird das konkrete Schadpotential in freier Wildbahn demonstriert, indem unter falscher Identität unerkannt auf elektronische Patientenakten zugegriffen sowie qualifizierte elektronische Signaturen erzeugt werden. Damit ist der Nachweis erbracht, dass derartige Angriffe auf das Video-Ident weder verhindert noch nachträglich erkannt werden. Aus der anschließenden Bewertung des notwendigen niedrigen Angriffspotentials folgt eine Empfehlung gegen den weiteren Einsatz des Video-Idents.

Hintergrund

Im Kontext des Video-Idents wird die Identität einer natürlichen Person durch eine Menge von Identitätsattributen wie Namen oder Geburtsdatum eindeutig beschrieben. Damit Dritte die Identität prüfen können und sich nicht auf eine bloße Behauptung verlassen müssen, muss durch die zu identifizierende Person ein Identitätsnachweis erbracht werden. In der Regel geschieht dies durch Vorlage eines staatlich herausgegebenen ID-Dokuments wie dem Personalausweis, welcher den Staat als Aussteller erkennen lässt und die Echtheitsprüfung anhand vielfältiger Sicherheitsmerkmale ermöglicht.

Wichtige Teilaspekte der Identitätsprüfung sind (Bundesamt für Sicherheit in der Informationstechnik, 2021):

1. Die zuverlässige Prüfung der ID-Dokumente. Hierbei werden die Authentizität und Integrität der relevanten ID-Attribute, beispielsweise das gedruckte Geburtsdatum, anhand taktil oder optisch überprüfbarer Sicherheitsmerkmale wie Hologrammen geprüft. Im Video-Ident wird anstelle des ID-Dokuments ein von der zu identifizierenden Person anzufertigendes Videobild dieses Dokuments geprüft.
2. Der zuverlässige Abgleich zwischen Person und ID-Dokument. Hierzu werden in der Regel direkt auf dem ID-Dokument aufgebrachte biometrische Referenzdaten mit biometrischen Charakteristika der zu identifizierenden Person abgeglichen. Im Video-Ident wird zumeist das im Videobild des ID-Dokuments sichtbare Passfoto mit dem im Videobild sichtbaren Gesicht der Person verglichen.
3. Die Sicherheit der dabei verwendeten Übertragungskanäle, sofern kein unmittelbarer Präsenzkontakt zur Person und kein unmittelbarer Zugriff auf das ID-Dokument besteht.

Spätestens seit die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in 2014 die Rechtsmeinung äußerte, wonach im Video-Ident von einer persönlichen Anwesenheit auszugehen sei und die bei einer Fernidentifizierung rechtlich vorgeschriebenen Sorgfaltspflichten somit umgangen werden können (Bundesanstalt für Finanzdienstleistungsaufsicht, 2014), werden vermehrt indirekte Identifikationsverfahren mittels Videoübertragung – kurz Video-Ident – eingesetzt, bei denen wie vorgenannt kein unmittelbarer Präsenzkontakt zur Person und kein unmittelbarer Zugriff auf das physische ID-Dokument bzw. den vorgelegten Sichtausweis besteht, der Prüfer das ID-Dokument sowie die zu überprüfende Person jedoch „über einen entfernten, üblicherweise audio-visuellen Kanal in Augenschein nehmen kann“ (Bundesamt für Sicherheit in der Informationstechnik, 2021).

Video-Ident wird als unsicher und unzulässig bewertet

Spätestens seit 2014 sind allerdings auch erhebliche Zweifel an der Vertrauenswürdigkeit des Video-Idents bekannt. So empfiehlt die damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit „auf die Möglichkeiten einer Videoidentifizierung zu verzichten“ und verweist auf die ungeklärte Wirksamkeit. Im Tätigkeitsbericht für 2013 – 2014 heißt es:

„Ob die Zuverlässigkeit der „Inaugenscheinnahme“ einer Person und ihres Ausweises mittels Videotechnik dem unmittelbaren persönlichen Kontakt gleichgestellt werden kann, erscheint mir mehr als fraglich. Über eine Videoverbindung können beispielsweise Sicherheitsmerkmale des Ausweises wie Hologramme nicht eindeutig als echt erkannt werden. Auch andere Manipulationen am Ausweis sind

nicht ohne weiteres so offensichtlich wie bei einer tatsächlichen Inaugenscheinnahme“ (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2015).

Im Tätigkeitsberichts 2017 – 2018 kommt der BfDI zu einer noch stärkeren Bewertung:

„Die Videoidentifizierung weist nicht das gleiche Sicherheitsniveau auf, wie die Identifizierung unter Anwesenden. Eine Dokumentenprüfung ist nach dem heutigen Stand der Technik in einem Videokanal nicht vollumfänglich möglich. Daher kann bei einer Videoidentifizierung noch schlechter als bei der Identifizierung vor Ort unterschieden werden, ob ein Ausweisdokument echt ist oder eine Fälschung vorliegt […]. Da die Integrität der zur Identifizierung herangezogenen Daten maßgeblich für jedwede sichere Identifizierungsmethode ist, bei der Videoidentifizierung aber nicht erfüllt werden kann, lehne ich diese Identifizierungsmethode ab.“ (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 2019)

Schließlich veröffentlicht der BfDI mit dem Tätigkeitsbericht 2020 eine Grundsatzentscheidung:

„Videoidentifizierungsverfahren sind risikobehaftet. Wo ein sehr hohes Vertrauensniveau erreicht werden muss, sind sie datenschutzrechtlich sogar unzulässig“. Dies gelte in Bereichen „in denen die Identifizierung ein sehr hohes Vertrauensniveau erfüllen muss“ wie beispielsweise „zum Schutz besonders schutzbedürftiger Kategorien von personenbezogenen Daten nach Artikel 9 DSGVO, wie etwa im Gesundheitswesen.“ (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 2021)

Spätestens seit 2017 ist die Angreifbarkeit des Video-Idents auch praktisch durch „Manipulation und Simulation des Ausweisdokuments auf videobearbeitungstechnischer Ebene“ unter „Verwendung von Standardkomponenten“ im Auftrag des BSI nachgewiesen und öffentlich bekannt (Bundesamt für Sicherheit in der Informationstechnik, 2017). Anschließend warnte das BSI vor dem weiteren Einsatz des Verfahrens: „Sicherheitsvorkehrungen bei Video-Ident könnten mithilfe von Bildmanipulationen sowie falschen oder gestohlenen persönlichen Daten ausgetrickst werden“ (BILD am SONNTAG, 2019).

Zuletzt hat die Firma Sensity B.V. ein Deepfake Offensive Toolkit (DOT) veröffentlicht und damit den Abgleich zwischen Person und ID-Dokument ebenfalls auf videobearbeitungstechnischer Ebene angegriffen (Sensity B.V., 2021) (Sensity B.V., 2022).

Dennoch Festhalten an Video-Ident

Entgegen der Grundsatzentscheidung des BfDI und der Warnung durch das BSI hält jedoch nicht nur die Bafin weiter am Video-Ident fest. Inzwischen wurde das Verfahren sogar in vielen weiteren Bereichen zur Identifikation natürlicher Personen eingeführt.

- Beispielsweise hat die BNetzA das Video-Ident zwischenzeitlich per Verfügung in verschiedenen Ausprägungen zur „Identifizierung einer natürlichen Person im Rahmen der Beantragung eines qualifizierten Zertifikates“ anerkannt (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 2018).
- Auch die Bundesregierung sieht im Video-Ident ein geeignetes Verfahren für den dauerhaften Zugriff auf Gesundheitsdaten: „Weiterhin ist die nachträgliche Identifikation beispielsweise unter Nutzung eines Video-Ident-Verfahrens […] möglich. Nach Kenntnis der Bundesregierung können auch Online-Ident-Verfahren die Voraussetzungen für eine solche sichere Identifizierung nach § 336 Fünftes Buch Sozialgesetzbuch (SGB V) erfüllen“ (Deutscher Bundestag, 2021).

- Zwischenzeitlich hat die gematik „die Nutzung des VideoIdent-Verfahrens ohne Operator (vollautomatisierte VideoIdent-Verfahren ohne Prüfung durch einen Mitarbeiter) zur nachträglichen Identifikation des Versicherten zugelassen“ (gematik GmbH, 2019).
- Zuletzt hat auch die BaFin das Video-Ident im Anwendungsbereich des Geldwäscherechts evaluiert und verlauten lassen, dass das Verfahren „als Brückentechnologie weiter fortgeführt“ werde (Bundesanstalt für Finanzdienstleistungsaufsicht, 2022).

Die Video-Ident-Anbieter bewerten die Sicherheit ihrer eigenen Verfahren weiterhin als hoch, ohne dafür Belege vorzubringen. Die Manipulation des Videobildes sei „aktuell kein wirtschaftlich sinnvoller Angriff“ (bitkom; vatm, 2021) (Abbildung 1). Einige Anbieter behaupten sogar, sie „haben bereits Gegenmaßnahmen gegen solche [im Auftrag des BSI demonstrierten] Angriffe implementiert“[1].

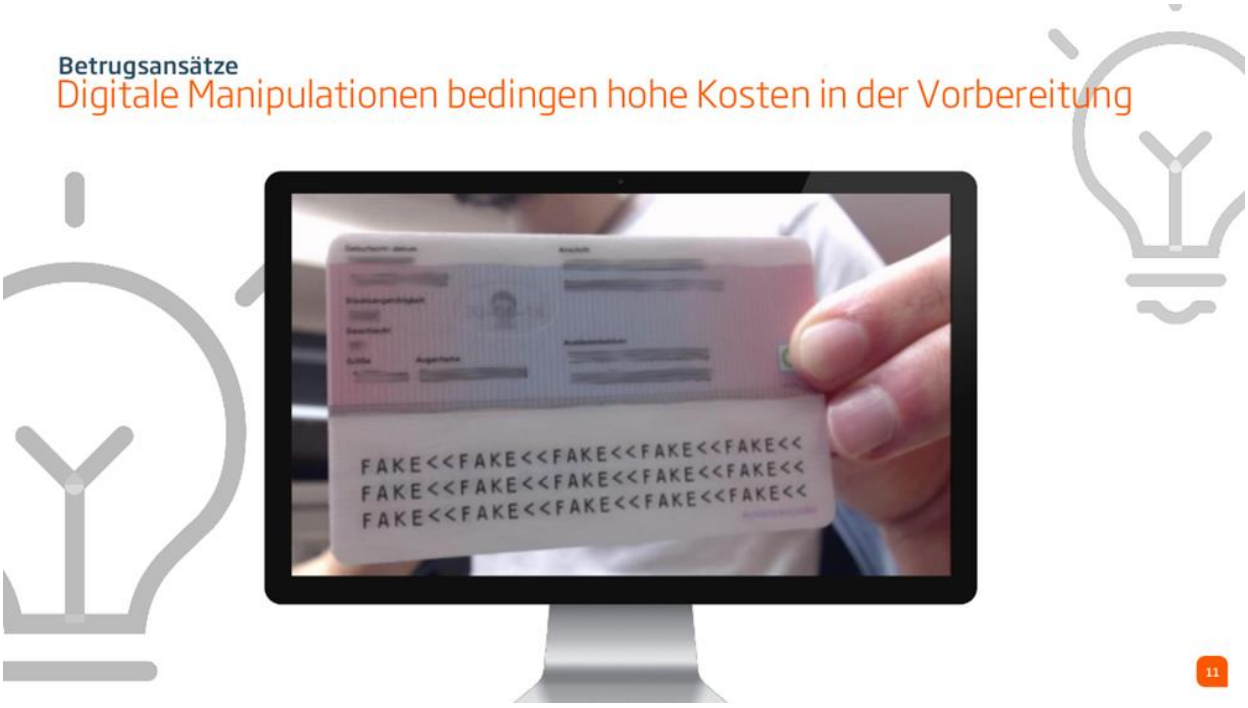

Abbildung 1: Laut IDnow bedingen digitale Manipulationen hohe Kosten in der Vorbereitung (IDnow GmbH, 2018).

Gefördert wird das Video-Ident auch aus dem Bundesministerium für Wirtschaft und Klimaschutz (Bundesministerium für Wirtschaft und Klimaschutz, 2020). Von Seiten der Wirtschaft wird betont, dass Video-Ident „einen Exportschlager darstelle“ (Wirtschaftsforum der SPD e.V., 2019).

Grundlegend für das weitere Festhalten an Video-Ident ist die u. a. von der Bundesregierung vorgebrachte Behauptung, dass das Video-Ident trotz bekannter Angriffsmöglichkeiten weiterhin eingesetzt werden könne – jedenfalls solange, bis „konkrete Sicherheitsvorfälle zur Kenntnis gelangt [sind], in denen mittels eines Hackerangriffs, also durch Manipulation des Video-Streams, eine unzutreffende Identifizierung der jeweiligen Person zu betrügerischen Zwecken erfolgt

[1] Antwort von Amin Bauer, Managing Director, Chief Technical Officer & Co-Founder der IDnow GmbH, auf den Vortrag zu Deep Faked Video Identity Manipulations (Herpers, Scherfgen, Jato, Millberg, & Hinkenjann, 2022), auf dem ENISA-ETSI Joint Workshop on Remote Identity Proofing am 3. Mai 2022 in München.

ist“ (Bundesregierung, 2019). Hierbei wird ein Schaden in Kauf genommen. Das Schadensausmaß ist umso größer, desto länger ein Angriff nicht zur Kenntnis gelangt.

Die gegenteiligen, negativen Bewertungen des Video-Idents u. a. seitens des BfDI und des BSI basieren demgegenüber auf der in Fachkreisen anerkannten Festlegung (Bundesamt für Sicherheit in der Informationstechnik, 2021), wonach ein Verfahren zur ID-Prüfung für das angestrebte Vertrauensniveau untauglich ist, sobald es einen möglichen Angriff gibt, der reproduzierbar funktioniert. Dass es solche Angriffsmöglichkeiten auf Video-Ident gibt, haben das BSI und zuletzt Sensity B.V. aufgezeigt.

Angriffsmöglichkeiten durch Videomanipulaton

Die auf technischer Manipulation des Videobildes beruhenden Angriffe nutzen aus, dass die Echtheitsprüfung des physischen ID-Dokuments sowie der zuverlässige Abgleich zwischen Person und ID-Dokument im Video-Ident lediglich anhand des Videobildes vorgenommen wird und nicht anhand des Originals. Das Videobild wird dabei unter Kontrolle der zu identifizierenden Person erzeugt, welche hier die Rolle des Angreifers einnimmt. Daraus folgt, dass der Prüfer eine Manipulation des Videobilds nicht verhindern kann. Er kann lediglich versuchen, diese Manipulation nachträglich zu erkennen. Auf die Prüfung der Sicherheitsmerkmale des echten ID-Dokuments muss der Prüfer dabei verzichten, lediglich die Videobilder einiger „im Weißlicht visuell zu erkennenden optischen Sicherheitsmerkmale“ (Bundesanstalt für Finanzdienstleistungsaufsicht, 2017) können zur Prüfung herangezogen werden. Nicht im Videobild erkennbar sind beispielsweise sehr feine optische Strukturen wie Guillochen und Mikroschriften, UV-Aufdrucke sowie Oberflächenprägungen (Abbildung 2). Taktile Sicherheitsmerkmale können im Video-Ident grundsätzlich nicht geprüft werden.

Abbildung 2: Laut BSI sind die meisten Sicherheitsmerkmale des Personalausweises im Video-Ident nicht prüfbar oder anfällig für Manipulation (Bundesamt für Sicherheit in der Informationstechnik, 2018).

Zu den im Videobild sichtbaren Merkmalen gehören insbesondere die Hologramme und weitere beugungsoptisch wirksame Strukturen. Diese werden zumindest in den regulierten Video-Ident-Verfahren geprüft (Bundesanstalt für Finanzdienstleistungsaufsicht, 2017) (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 2018). Eine Manipulation des Videobildes eines ID-Dokuments muss demnach die beugungsoptisch wirksamen Sicherheitsmerkmale erhalten oder nachbilden, um unerkannt zu bleiben (Abbildung 3) (Abbildung 4).

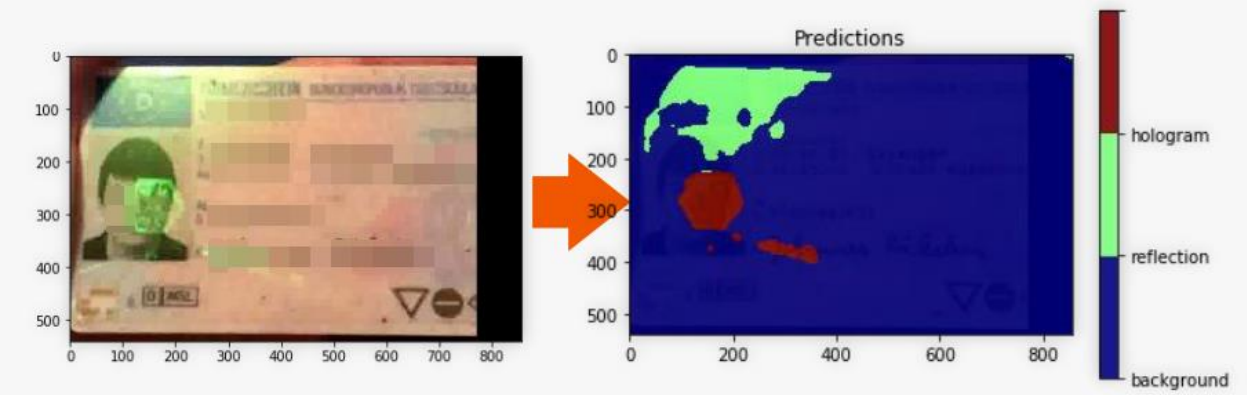

Abbildung 3: Hologrammerkennung mittels Segmentierung nach IDnow (IDnow GmbH, 2019).

Abbildung 4: Hologrammerkennung mittels Segmentierung nach Nect (Nect GmbH, 2019).

Vito-Studie

Das Institut für Visual Computing (IVC) der Hochschule-Bonn-Rhein-Sieg hat bereits 2017 in einer vom BSI beauftragten Studie einen Angriff auf die Echtheitsprüfung des ID-Dokuments im Video-Ident aufgezeigt. Dabei wird das Videobild eines einfachen Farbdrucks bzw. einer Vollfälschung eines ID-Dokuments mit computergenerierten Hologrammen überlagert (Abbildung 5). Damit ist die Angreifbarkeit des Video-Idents durch „Manipulation und Simulation des Ausweisdokuments auf videobearbeitungstechnischer Ebene“ unter Einsatz von „Standardkomponenten“ belegt (Bundesamt für Sicherheit in der Informationstechnik, 2017). Nach Angaben des BSI hält das Video-Ident dabei nicht einmal moderatem Angriffspotential stand. „Optische Sicherheitsmerkmale können nicht sicher digitalisiert werden“ (Bundesamt für Sicherheit in der Informationstechnik, 2018).

In einer Weiterentwicklung des Angriffs werden von Fingern überdeckte Segmente des unechten ID-Dokuments im Videobild mittels eines auf synthetisch erzeugten Daten trainierten Convolutional Neural Network erkannt. Lediglich die nicht von Fingern überdeckten Segmente werden anschließend mit den computergenerierten Sicherheitsmerkmalen überlagert (Abbildung 6).

Die Studie hatten keinen Einfluss auf die weitere Verbreitung des Video-Idents, auch weil das BSI in Folge zwar gegenüber Boulevardmedien vor Video-Ident gewarnt (BILD am SONNTAG, 2019), aber keine Warnung im Sinne von i. S. v. § 7 Absatz 1 lit. a) des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik ausgesprochen hatte (Bundesregierung, 2019).

Abbildung 5: Aufbringen computergenerierter Hologramme auf das Videobild einfacher vollgefälschter ID-Dokumente in einer Studie des IVC im Auftrag des BSI (Herpers, Scherfgen, Jato, Millberg, & Hinkenjann, 2022).

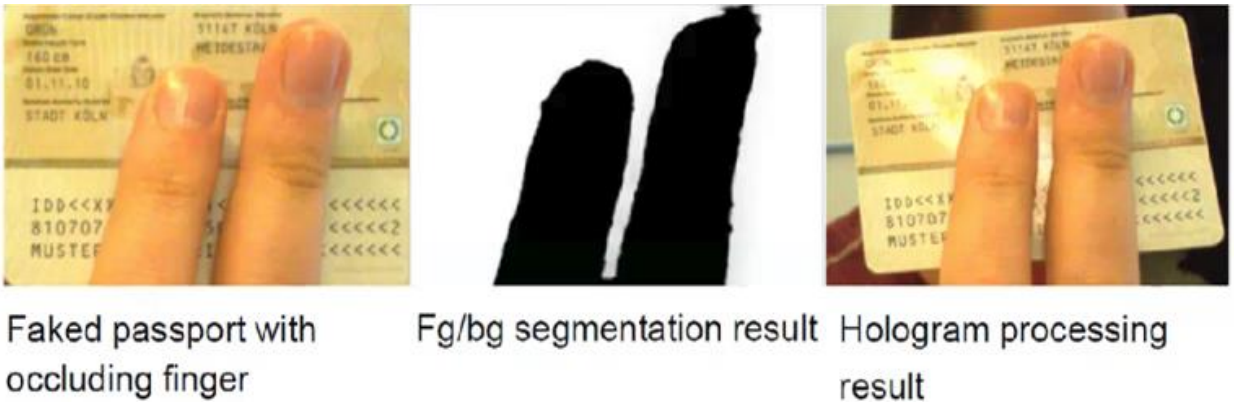

Abbildung 6: Segmentierung des ID-Dokuments in einer Studie des IVC (Herpers, Scherfgen, Jato, Millberg, & Hinkenjann, 2022).

Deepfake Offensive Toolkit

Die Firma Sensity B.V. hat wiederholt einen Angriff auf den Abgleich zwischen ID-Dokument und Person demonstriert (Sensity B.V., 2021) (Sensity B.V., 2022). Dabei wird das Gesicht der zu identifizierenden Person im Videobild durch das Gesicht der im biometrischen Passfoto dargestellten Person ersetzt. Die in Echtzeit berechneten Deep-Fakes „können die Bewegungen der Gesichtsmerkmale der Angreifer originalgetreu reproduzieren […] selbst wenn sich die Gesichtszüge, z. B. Augenform und -farbe, die Höhe der Wangenknochen oder die Form des Mundes ändern [...]“ (Sensity B.V., 2022). Im Ergebnis waren ein halbes Jahr nach erster Veröffentlichung weiterhin 9 von 10 der getesteten Video-Ident-Verfahren, die unter anderem von Banken eingesetzt werden, verwundbar (Sensity B.V., 2022).

Auch diese Veröffentlichung hatte keinen Einfluss auf die weitere Verbreitung des Video-Idents; insbesondere hat sie keinen Eingang in die Regulatorik gefunden. Im Ergebnis der Evaluierung des Video-Idents der BaFin blieb sie unberücksichtigt (Bundesanstalt für Finanzdienstleistungsaufsicht, 2022).

Neuer vereinfachter Angriff

Nachfolgend wird ein neuer vereinfachter Angriff auf Video-Ident beschrieben, der ebenfalls auf technischer Manipulation des Videobildes beruht. Dieser zielt auf den Teilaspekt der zuverlässigen Prüfung der ID-Dokumente.

Art des Angriffs, Voraussetzungen und Ziele

Der Angriff basiert auf der videotechnischen Kombination zweier oder mehrerer echter ID-Dokumente im Videobild zu einem künstlichen neuen ID-Dokument. Dazu werden Bildausschnitte aus einem Video in ein zweites Video übertragen.

In einer möglichen Ausprägung wird ein biometrisches ID-Attribut – beispielsweise das biometrische Passbild – des ersten ID-Dokuments (Ziel-Dokument) im Videobild in Echtzeit durch das passende biometrische ID-Attribut des zweiten ID-Dokuments (Quell-Dokument) ersetzt. Der Inhaber des Quell-Dokuments kann sich anschließend im Video-Ident mit dem Ziel-Dokument ausweisen, ohne dass der biometrische Abgleich zwischen Person und ID-Dokument fehlschlägt.

In einer weiteren möglichen Ausprägung wird ein nicht-biometrisches ID-Attribut – beispielsweise die Anschrift – auf einem ersten ID-Dokument (Ziel-Dokument) im Videobild durch das passende ID-Attribut eines zweiten ID-Dokuments (Quell-Dokument) ersetzt. Der Inhaber des Ziel-Dokuments kann sich anschließend im Video-Ident mit dem Ziel-Dokument und videotechnisch ersetztem ID-Attribut ausweisen.

Je nach Motivation des Angreifers kann der Angriff darauf abzielen, eine beliebige neue Identität zu erschaffen (z. B. Betrug, Geldwäsche, Bankdrop) oder eine bestehende Identität zu übernehmen (z. B. Zugriff auf bestehende Konten, Patientenakten).

Voraussetzung zur Schaffung einer beliebigen neuen Identität ist der Besitz eines eigenen ID-Dokuments und beliebiger weiterer ID-Dokumente der gleichen Art.

Voraussetzung zur Übernahme einer bestehenden Identität ist ebenfalls der Besitz eines eigenen ID-Dokuments und ganz bestimmter weiterer ID-Dokumente der gleichen Art. Diese weiteren ID-Dokumente müssen in Kombination die für den Identitätsdiebstahl notwendigen ID-Attribute ergeben.

Der geringste Aufwand entsteht dem Angreifer, wenn er für die Vorbereitung des Angriffs kurzzeitig in den Besitz des ID-Dokuments der angegriffenen Person selbst gelangt – mögliche Szenarien sind beispielsweise das Auffinden eines verloren gegangenen ID-Dokuments oder der Zugriff auf das ID-Dokument eines Mitarbeiters am Arbeitsplatz.

Vorgehensweise

Zunächst wird das Quell-Dokument auf einem ArUCo-Markerboard (S. Garrido-Jurado, 2014) fixiert und aus möglichst vielen Winkeln unter konstanten Beleuchtungsbedingungen von einer feststehenden Kamera in einem Video aufgenommen, die auch später für den Angriff verwendet werden soll. Dabei wird der Mittelpunkt des ID-Dokuments mit der Kamera fokussiert und das Markerboard mit dem ID-Dokument gegenüber der Kamera um die Längs- und Querachse um bis zu 90° gekippt (Abbildung 7).

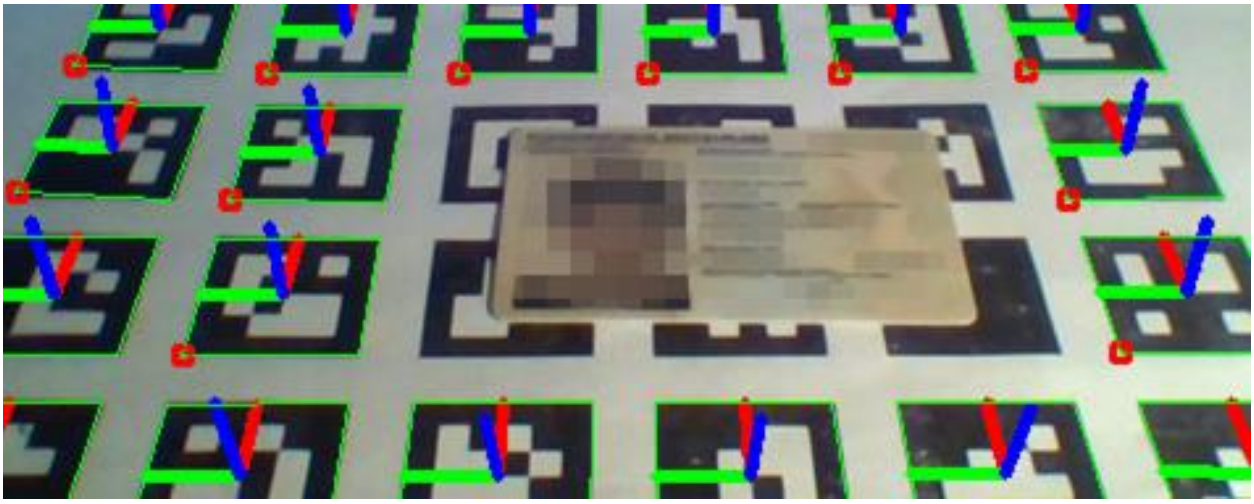

Abbildung 7: Aufnahme der SVBRDF (Weyrich, Lawrence, P. A. Lensch, Rusinkiewicz, & Zickler, 2009) des ID-Dokuments.

Aus den Einzelbildern des Videos wird anschließend das ID-Dokument freigestellt und perspektivisch entzerrt. Im Ergebnis liegen nun rektifizierte Aufnahmen des Quell-Dokuments aus allen relevanten Kamerawinkeln vor (Abbildung 8).

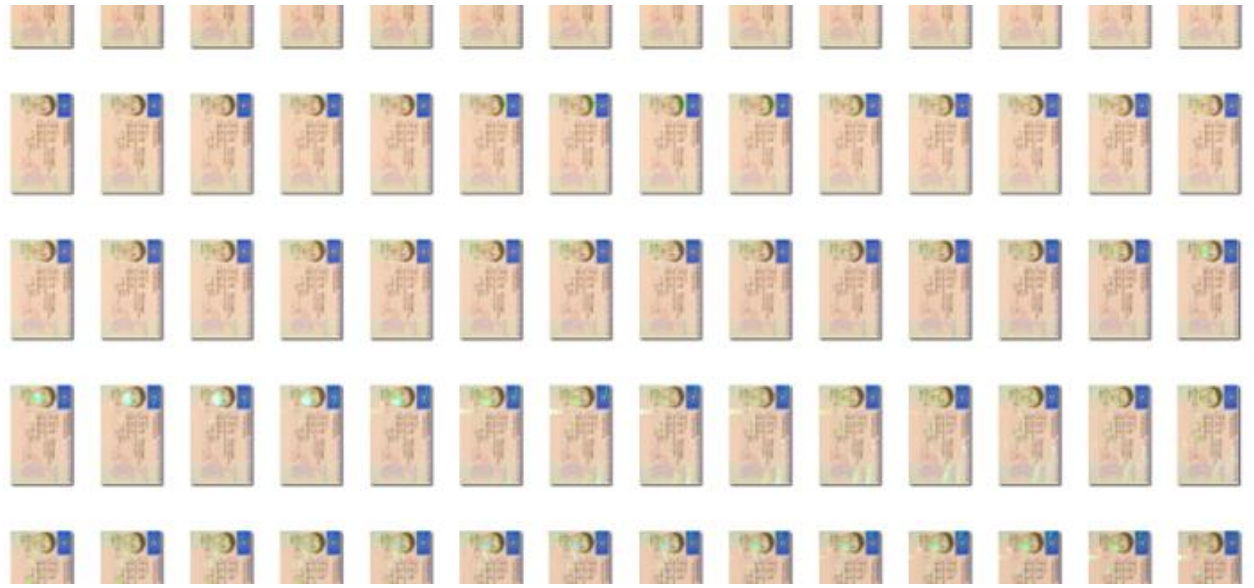

Abbildung 8: Perspektivisch entzerrte Einzelbilder des ID-Dokuments zur Approximation der SVBRDF eines Führerscheins unter konstanter Beleuchtung.

Die vom Quell-Dokument auf das Ziel-Dokument zu übertragenden Bildausschnitte, beispielsweise ein Ausschnitt des biometrischen Fotos, werden anschließend händisch durch einmaliges Zeichnen einer Bildmaske ausgewählt (Alpha-Channel-Maske) (Abbildung 9).

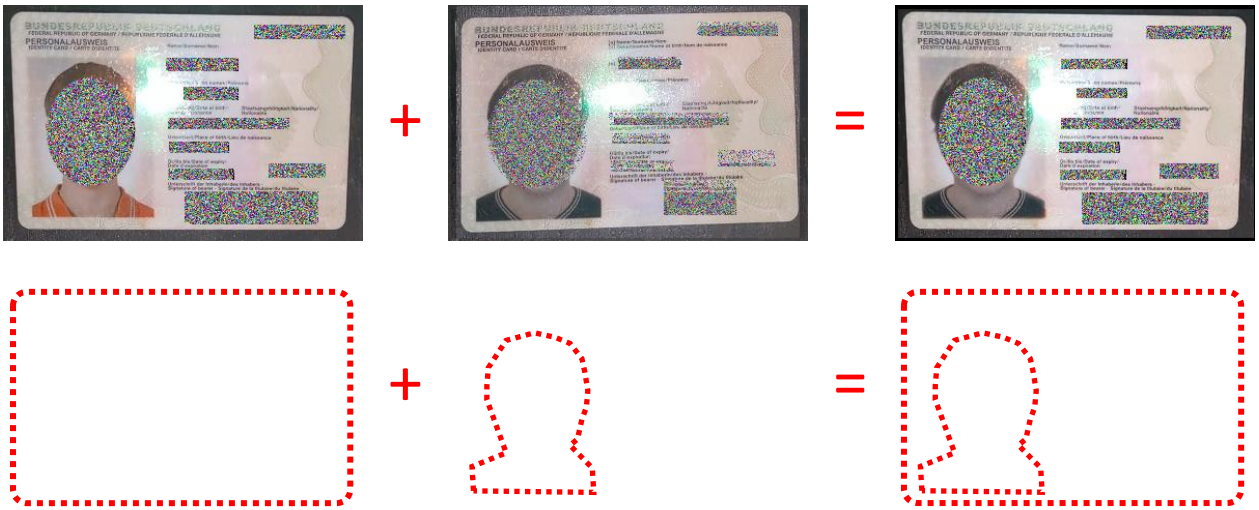

Abbildung 9: Übertragung eines ausgewählten bzw. maskierten Bildausschnitts des Quell-Dokuments auf das Ziel-Dokument - hier das biometrische Passbild.

Nach Abschluss der vorbereitenden Maßnahmen kann das Video-Ident initiiert werden. In dessen Verlauf wird die zu identifizierende Person gebeten, ihr ID-Dokument in die Kamera zu halten. Hierzu wird das Ziel-Dokument verwendet. Dieses wird im Videobild mittels Speeded Up Robust Features (SURF) (Bay, Tuytelaars, & Van Gool, 2006) erkannt und eine Homographie (Kriegman, 2007) berechnet, welche die Bild-Ausschnitte des Quell-Dokuments auf das Ziel-Dokument abbildet. Das so manipulierte Videobild wird dann auf einem handelsüblichen Fernseher wiedergegeben. Das Fernsehbild wird unter Beibehaltung der ursprünglichen optischen Achse abgefilmt und an den Video-Ident-Anbieter übertragen (Abbildung 10) (Abbildung 11).

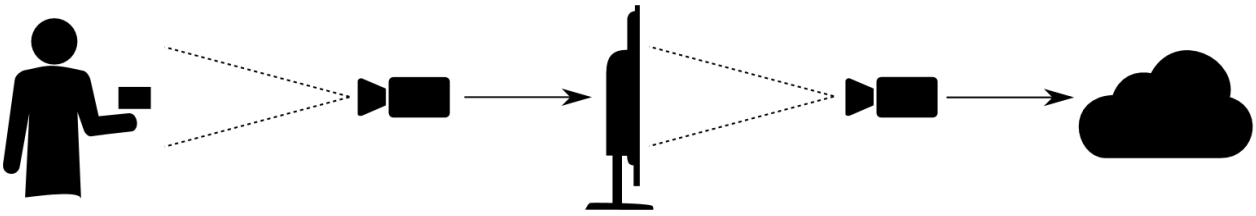

Abbildung 10: Das manipulierte Videobild wird auf einem handelsüblichen Fernseher wiedergegeben und dort erneut abgefilmt.

Bei der videotechnischen Übertragung eines ID-Attributes aus dem Videobild des Quell-Dokuments in das Videobild des Ziel-Dokuments werden auch die über diesem ID-Attribut im Weißlicht sichtbaren optischen Sicherheitsmerkmale, insbesondere Hologramme, übertragen. Bei der Auswahl der zu übertragenden ID-Attribute bzw. des Bildausschnitts sollte daher darauf geachtet werden, dass sich darüber liegende Hologramme möglichst nahtlos in das Ziel-Dokument einfügen.

Ähnliches gilt, wenn ID-Attribute an weiterer Stelle auf dem Ziel-Dokument erneut holographisch wiedergegeben werden. Wird beispielsweise das biometrische Passbild manipuliert, so muss auch dessen holographische Wiedergabe an anderer Stelle – beim neuen Personalausweis das sog. Identigram – manipuliert werden.

In der Praxis hat sich allerdings herausgestellt, dass im Video-Ident zwar die Existenz von Hologrammen an der erwarteten Stelle geprüft wird, eine inhaltliche Prüfung allerdings nicht oder nur unzureichend stattfindet, sodass auf die zwei vorgenannten Schritte derzeit verzichtet werden kann.

Ebenfalls ist auf die Konsistenzprüfung der ID-Attribute zu achten. Wird beispielsweise der Name im Videobild manipuliert, so müssen auch Teile der maschinenlesbaren Zone im Videobild manipuliert werden. Andernfalls würde die Ersetzung mit Abgleich der maschinenlesbar übertragenen Daten leicht auffallen.

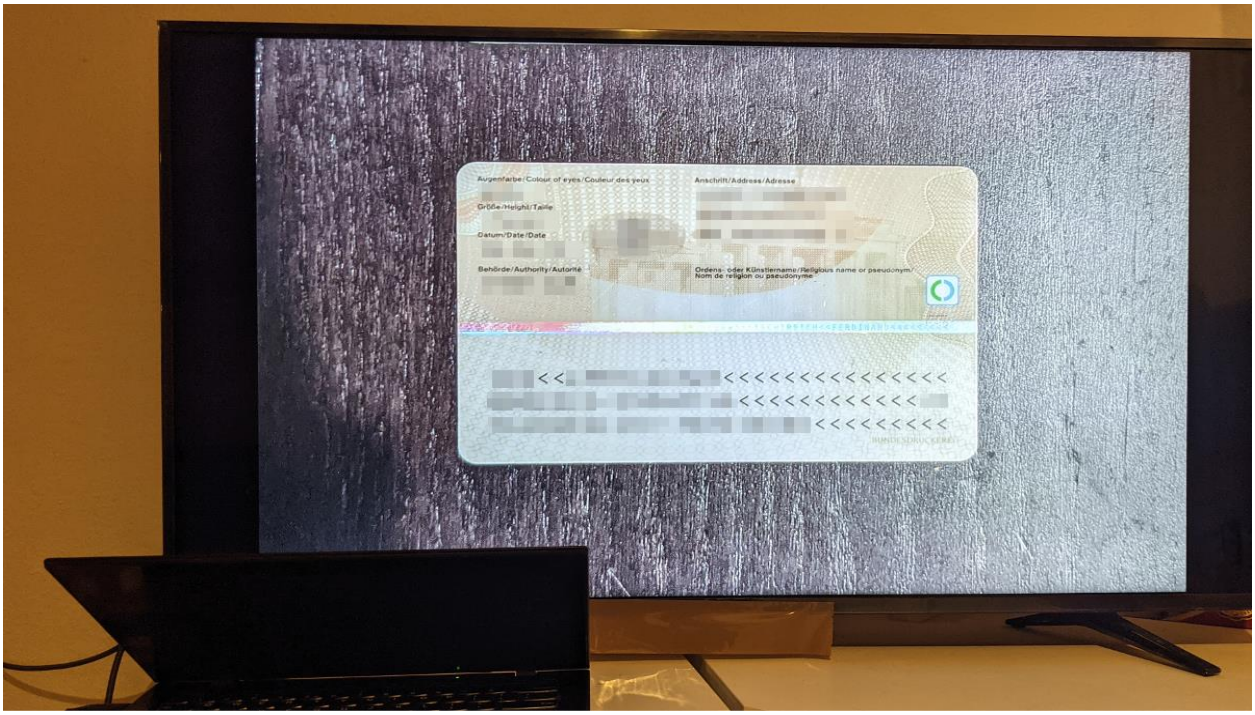

Abbildung 11: Zum Einsatz kommt preisgünstige Verbraucherelektronik.

Vorgehensweise bei Echtheitsprüfung mit Frontkamera

Im Video-Ident wird gelegentlich die Abdeckung von bestimmten Bereichen des Ziel-Dokuments durch einen oder mehrere Finger verlangt, während die zu identifizierenden Person das Dokument und sich selbst mit der Frontkamera am Smartphone oder der klassischen Webcam filmt. Dies ist beispielsweise bei allen Video-Ident-Verfahren der Fall, die den Vorgaben der BaFin genügen (Bundesanstalt für Finanzdienstleistungsaufsicht, 2017). Ziel ist es, damit eine Manipulation des Videobildes aufzudecken. Derart abgedeckte Bereiche des Ziel-Dokuments dürfen nicht von den gewichteten Bildausschnitten des Quell-Dokuments überlagert werden und müssen daher maskiert werden. Die von Fingern überdeckten Segmente des ID-Dokuments im Videobild können mit einer einfachen Methode erkannt werden. Zunächst werden die Finger mit roter wasserlöslicher Aquarellfarbe eingefärbt. Anschließend wird das Videobild mittels Schwellenwertverfahren anhand des roten Farbtons (Hue) segmentiert. Es erfolgt eine automatisierte Nachbearbeitung des Randpolygons (Interpolation und Glättung). Die ursprüngliche Hautfarbe wird anschließend durch Verschiebung des Farbtons innerhalb des Segmentes wiederhergestellt (Abbildung 12).

Abbildung 12: Segmentierung anhand rot eingefärbter Bereiche. Die Original-Hautfarbe wird durch Verschiebung des Farbtons innerhalb des Segmentes wiederhergestellt.

Vorgehensweise bei Echtheitsprüfung mit Rückkamera

Einige Video-Ident-Verfahren verlangen eine Nahaufnahme des ID-Dokuments mit der Smartphone-Rückkamera bei eingeschalteter Rückkamera-LED. In diesem Fall kann die beschriebene Vorgehensweise weiter vereinfacht werden. Dabei werden das Quell-Dokument und das Ziel-Dokument mit identischem Winkel zur Kamera nebeneinandergelegt und mit eingeschalteter Rückkamera-LED abgefilmt. Wie zuvor wird der vom Quell-Dokument auf das Ziel-Dokument zu übertragende Bildausschnitt mittels Maske (Alpha-Channel-Maske) ausgewählt und anhand der mit Hilfe von SURF berechneten Homographie auf das Ziel-Dokument übertragen (Abbildung 13).

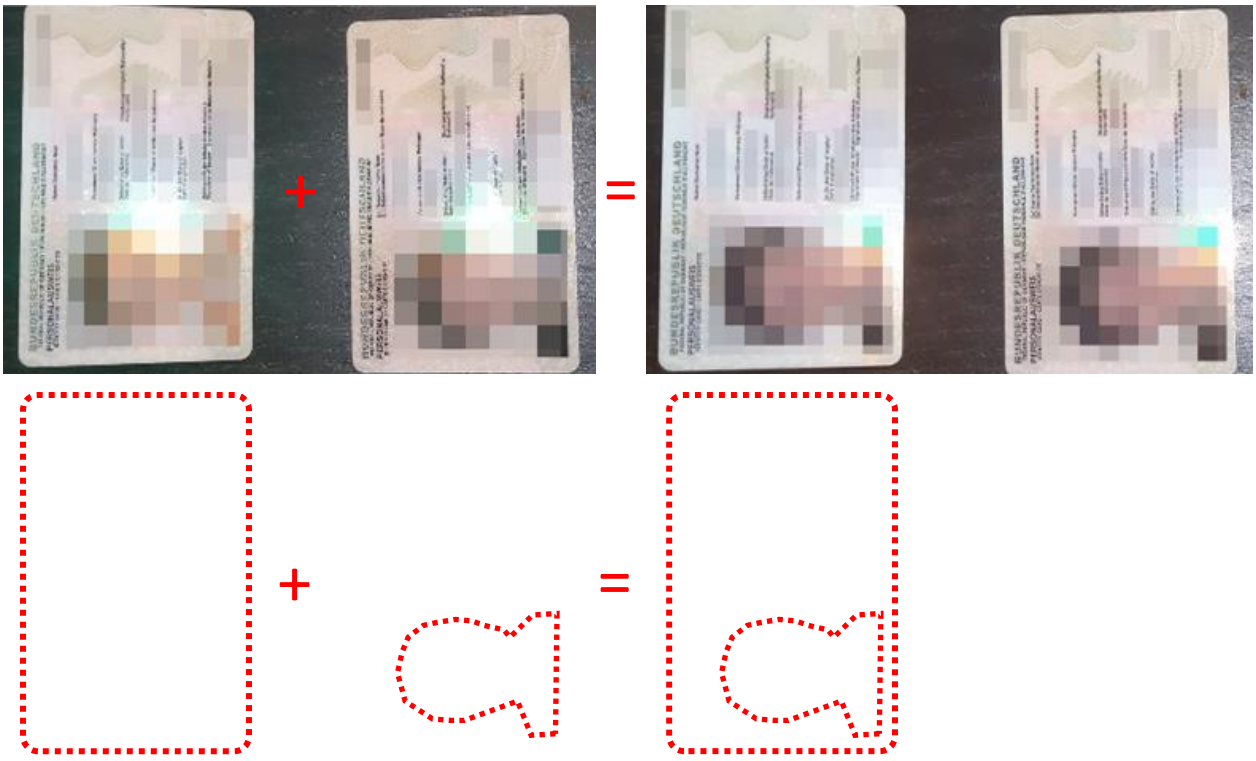

Abbildung 13: Übertragung eines ausgewählten bzw. maskierten Bildausschnitts des Quell-Dokuments auf das Ziel-Dokument – hier nach vereinfachter Vorgehensweise bei Echtheitsprüfung mit Rückkamera.

Praktische Demonstration

In einer praktischen Demonstration des Angriffs konnten die Video-Ident-Verfahren von mehr als sechs verschiedenen inner- und außereuropäischen Video-Ident-Anbietern überwunden werden.

Angriff auf die elektronische Patientenakte

Rund 73 Millionen gesetzlich Krankenversicherte in Deutschland haben einen gesetzlichen Anspruch auf die Überführung ihrer in Arztpraxen und weiteren Leistungserbringerinstitutionen gespeicherten Gesundheitsdaten in eine elektronische Patientenakte (ePA) nach § 341 SGB V. Dort werden die Daten dann zentral, lebenslang fach- und einrichtungsübergreifend gespeichert. Der Zugang zur ePA ist nach § 336 Absatz 5 SGB V nur nach einer sicheren Identifikation des Versicherten möglich. Von den 30 größten Krankenkassen haben zum Zeitpunkt der Demonstration 29 Kassen die Identifikation des Versicherten per Video-Ident angeboten. Eine Kasse verzichtete auf die gesetzlich vorgeschriebene Identifikation.

In einem ersten Schritt wurde ein ID-Dokument eines gesetzlich Versicherten, der bisher keine ePA beantragt hatte, wie zuvor beschrieben abgefilmt. Zudem lag dessen Krankenversichertennummer vor.

In einem zweiten Schritt wurde für den Versicherten unter Angabe dieser Daten sowohl ein Zugang zur Online-Geschäftsstelle von dessen Krankenkasse als auch eine ePA beantragt und die dabei eingesetzte „Videoidentifizierung mit automatisiertem Verfahren“ mit der zuvor beschriebenen Vorgehensweise überwunden.

In einem dritten Schritt wurden für den Versicherten über die Online-Geschäftsstelle eine Patientenquittung nach § 305 SGB V angefordert und die dort genannten Leistungserbringer gebeten, Behandlungsunterlagen in die ePA einzustellen, nachdem diesen Leistungserbringern zuvor die Berechtigung für den Zugriff auf die ePA des Versicherten erteilt wurde.

Im Ergebnis konnte Zugriff auf weitreichende Gesundheitsdaten des Versicherten, darunter eingelöste Rezepte, Arbeitsunfähigkeitsbescheinigungen, ärztliche Diagnosen sowie Original-Behandlungsunterlagen genommen werden.

Angriff auf digitale Signaturen und weitere Anwendungen

Die Wirksamkeit der beschriebenen Angriffsvarianten wurde anschließend gegen die Video-Ident-Verfahren von sechs weiteren inner- und außereuropäischen Anbietern demonstriert. Im Zuge dessen wurde bei einer Videoidentifizierung mit menschlichem Operator ein Datenleck festgestellt, worüber signierte Kundendokumente – darunter Kreditverträge von Privatverbrauchern – zugänglich waren. Solche Dokumente beinhalten neben allgemeinen persönlichen Daten wie Namen, Anschrift, Geburtsdatum, Familienstand, Wohnsituation usw. auch Angaben zum aktuellen Arbeitgeber, Einkommen, Rente, Unterhalt, Miete, Krediten, Restschulden, Raten, Zahlungsplänen und mehr.

Die Angriffe gegen die Video-Ident-Verfahren wurden in jedem Fall mit Einwilligung der betroffenen Person durchgeführt. In jedem Fall waren die unangekündigt durchgeführten Angriffe erfolgreich; in keinem Fall gelangten die Angriffe den Verfahrensverantwortlichen zur Kenntnis – die darüber eröffneten Zugänge wurden bis zum Zeitpunkt dieser Veröffentlichung nicht gesperrt. Dies galt auch dann, wenn die Verfahrensverantwortlichen zuvor explizit auf das nachgewiesene Risiko im Zusammenhang mit Video-Ident sowie das konkrete Angriffsszenario hingewiesen wurden.

In mehreren Fällen wurde nach Durchführung der Angriffe auf Grundlage von Artikel 15 Abs. 1 DSGVO Auskunft über das vom Video-Ident-Anbieter aufgezeichnete Bildmaterial angefordert. In einem Fall waren auf dem Bildmaterial durch die Videomanipulation entstandene Artefakte erkennbar, die jedoch nicht zu einer Erkennung des Angriffs geführt haben (Abbildung 14).

Abbildung 14: Artefakte an der unteren linken Ecke eines Hologramms durch Abweichungen in dessen Positionierung auf dem Quell- und Ziel-Dokument (links); diese Artefakte verschwinden nach manueller Positionskorrektur. Artefakte durch Abfilmen von einem Fernsehbildschirm (rechts); diese Artefakte verschwinden bei Abfilmen von einem Videoprojektor.

Im Rahmen der Angriffe wurden folgende videotechnische Manipulationen am Videobild des ID-Dokuments durchgeführt: Manipulation der Anschrift, Manipulation des Passfotos und der Anschrift, sowie alleinige Manipulation des Passfotos.

Diskussion

Mit entsprechendem Aufwand kann jede ID-Prüfung überwunden werden. Ob ein Verfahren zur ID-Prüfung ein bestimmtes Vertrauensniveau erreicht, entscheidet sich daher nicht allein anhand der bloßen Existenz eines Angriffs. Relevant ist vielmehr der zur Durchführung des Angriffs notwendige Aufwand bzw. das notwendige Angriffspotential:

„Wurde ein erfolgreicher Angriff auf ein Verfahren zur ID-Prüfung praktisch umgesetzt oder theoretisch[2] identifiziert, so ist zu bewerten, ob er für die konkrete Anwendung bzw. das angestrebte Vertrauensniveau relevant ist". (Bundesamt für Sicherheit in der Informationstechnik, 2019)

Damit ein Verfahren zur ID-Prüfung ein substantielles Vertrauensniveau erreichen kann, muss es moderatem Angriffspotential widerstehen. Normales Vertrauensniveau erreicht ein Verfahren, welches dem Angriffspotential „enhanced-basic" widersteht (Bundesamt für Sicherheit in der Informationstechnik, 2019).

Das Angriffspotential des demonstrierten Angriffs bestimmt sich aus den Faktoren Zeit, Expertenwissen, Insiderkenntnisse, Zugangs- und Zugriffsgelegenheiten sowie Ausrüstung (Common Criteria, 2017). Im vorliegenden Fall ist davon auszugehen, dass auch Laien den Angriff unter Anleitung nach der beschriebenen Vorgehensweise durchführen können. Da dies aber nicht nachgewiesen ist, wird Expertenwissen vorausgesetzt. Alle zur Vorbereitung notwendigen Informationen waren öffentlich zugänglich, inklusive Informationen über die ausgenutzte Schwachstelle selbst. In der demonstrierten Angriffsvariante auf die elektronische Patientenakte bestand Zugriff auf das ID-Dokument der angegriffenen Person und deren Krankenversichertennummer. Je nach Ansicht, ob es sich dabei um eine beliebige oder eine bestimmte Person handelte, sind die notwendigen Zugangs- oder Zugriffsgelegenheiten mit „einfach" bis „moderat" zu bewerten (Bundesamt für Sicherheit in der Informationstechnik, 2021). Der zur erfolgreichen Durchführung des Angriffs notwendige Zeiteinsatz lag zwischen einer und zwei Wochen. Die Ausrüstung beschränkte sich hardwareseitig auf preisgünstige Verbraucherelektronik sowie rote Wasserfarbe, softwareseitig wurde auf die quelloffene Programmbibliothek OpenCV (Bradski, 2000) zurückgegriffen. In der Gesamtbewertung liegt das zur erfolgreichen Durchführung des Angriffs notwendige Angriffspotential damit bei „enhanced-basic" (Bundesamt für Sicherheit in der Informationstechnik, 2019) (Common Criteria, 2017).

Das Ergebnis steht damit im Einklang zur Feststellung des BSI, wonach Fälschungen, die einer „indirekten" ID-Prüfung mit einem Video-Ident-Verfahren standhalten, „weniger aufwändige Ausrüstung, […] weniger einschränkende Zugangs- / Zugriffsgelegenheiten, […] ein geringeres Maß an Insiderkenntnissen, […] ein geringeres Maß an Expertise" und damit insgesamt „ein geringeres Angriffspotential für ihre Erstellung benötigen" (Bundesamt für Sicherheit in der Informationstechnik, 2021).

Nach BSI TR-03147 Kapitel 2.4 „Berücksichtigung und Bewertung des Angriffspotentials" (Bundesamt für Sicherheit in der Informationstechnik, 2021) erreicht das Verfahren damit weder substantielles noch normales Vertrauensniveau. Die in BSI TR-03147 Kapitel 1.1 „Zielsetzung und Inhalt der Technischen Richtlinie" genannten Mindestanforderungen für das eIDAS-Vertrauensniveau „niedrig" (Bundesamt für Sicherheit in der Informationstechnik, 2019) werden nicht erfüllt. Es ist davon auszugehen, dass die

[2] „Sofern hinreichend empirisch oder theoretisch abgesichert, können potentielle Angriffe auch ohne (vollständige) praktische Durchführung bewertet werden." (Bundesamt für Sicherheit in der Informationstechnik, 2021)

angreiferseitig notwendige Expertise und die einzusetzende Zeit durch die vorliegende Veröffentlichung abzusenken sind, wodurch das notwendige Angriffspotential weiter sinkt.

Einschränkungen

Vorliegend nicht bewertet wurde die rechtliche Zulässigkeit des Video-Idents. So hat zuletzt der Bundesgerichtshof (BGH) mit Beschluss 4 Ars 14/19 die Notwendigkeit der „Vorlage der Urschrift des Ausweispapiers“ anstelle der elektronischen Kopie begründet „jedenfalls in denjenigen Fällen, in denen der Identität der Person für das Rechtsgeschäft eine herausgehobene Bedeutung zukommt“, insbesondere „bei notariell zu beurkundenden Rechtsgeschäften sowie Rechtsgeschäften im Anwendungsbereich des Geldwäschegesetzes“.

Bewertung der Ergebnisse

Mit der praktischen Demonstration des Angriffs konnte gezeigt werden, dass zentrale Annahmen hinsichtlich der Sicherheit des Video-Idents gegenüber Manipulation des Videobildes nicht haltbar sind: Der demonstrierte Angriff ist zum einen wirtschaftlich durchführbar, zum anderen konnten alle implementierten Gegenmaßnahmen unerkannt überwunden werden.

Angesichts des enormen technischen Fortschritts hinsichtlich der Angriffe mittels Deep-Fake und der Fokussierung allfälliger Gegenmaßnahmen hierauf ist festzuhalten, dass nicht nur das Gesicht der zu identifizierenden Person, sondern bereits die optische Sicherheitsmerkmale des ID-Dokuments nicht sicher digitalisiert werden können. Im Gegensatz zu Angriffen auf die Vor-Ort-Identifikation, für die ein Angreifer lokal vor Ort persönlich erscheinen und sein ID-Dokument im Original vorlegen muss, ist der demonstrierte Angriff auf Video-Ident in gewissem Rahmen skalierbar[3], weltweit anwendbar und nur schwer oder gar nicht rückverfolgbar.

[3] „Die Grenzkosten sowie das notwendige Know-how für die (wiederholte) Durchführung [eines Angriffs mittels video-/informationstechnischer Manipulation] sind vergleichsweise gering“. Daraus folgt eine „hohe Skalierbarkeit“ (Bundesamt für Sicherheit in der Informationstechnik, 2021).

Fazit

Entgegen der Grundsatzentscheidungen des BfDI und gegen die Empfehlung des BSI wird das Video-Ident-Verfahren weiter und vermehrt dort eingesetzt, wo für Institutionen, Patienten, Kreditnehmer, Versicherte und weitere Betroffene ein hohes Schadpotential besteht.

- Die Strategie abzuwarten, bis „konkrete Sicherheitsvorfälle zur Kenntnis“ gelangen (Bundesregierung, 2019), ist nicht aufgegangen. Die demonstrierten Angriffe sind nachweislich nicht zur Kenntnis gelangt.
- Die Annahme, dass moderne Video-Ident-Verfahren die bekannten Schwächen „durch den Einsatz von künstlicher Intelligenz“ überwinden und gar „einen besseren Prüfungsschutz“ bieten können (Techniker Krankenkasse, 2022), hat sich in der Praxis als falsch herausgestellt.

Um weiteren Schaden abzuwenden, besteht dringender Handlungsbedarf.

- Substantielles Vertrauensniveau kann bei Verifikation physischer ID-Dokumente aus der Ferne nicht erreicht werden. Sofern eine Identifikation tatsächlich notwendig ist, kann auf ein elektronisches ID-Dokument oder eine Vor-Ort-Identifikation zurückgegriffen werden.
- Gleiches gilt bei Verifikation biometrischer Merkmale aus der Ferne. Derzeit stehen „keine zuverlässigen Methoden zur Erkennung von Präsentationsangriffen in diesem Szenario zur Verfügung“ (Bundesamt für Sicherheit in der Informationstechnik, 2019). Die Angreifbarkeit sowie die Unwirksamkeit von Gegenmaßnahmen ist auch hier belegt (Sensity B.V., 2022).
- Mittels Video-Ident durchgeführte Identitätsfeststellungen sind je nach Schutzbedarf und Risiko erneut mit geeigneten Verfahren durchzuführen (Europäische Kommission, 2019).
- Festlegungen auf EU-Ebene sind notwendig, da EU-Anbieter „aufgrund des gemeinsamen Marktzugangs […] ihre Dienste auch in Deutschland anbieten“ (bitkom, 2018).
- Weitere Forschung ist notwendig, um bisher unberücksichtigte Angriffe zu identifizieren. „Angriffe auf das Ausweisdokument“ werden regelmäßig unberücksichtigt gelassen, so auch in der jüngsten Studie zu Angriffen und Gegenmaßnahmen in der Fernidentifizierung der ENISA (European Union Agency for Cybersecurity, 2022). Insbesondere bedarf jede Aussage zur Wirksamkeit von Gegenmaßnahmen gesicherter Evidenz.
- Für die Bewertung von Video-Ident-Verfahren fehlen neben „Sicherheits-, Zuverlässigkeits-, Qualitätskennzeichen“ insbesondere Referenzwerte, an denen sich ein Zulassungsverfahren orientieren könnte (TÜV TRUST IT, 2022). Die Erfüllung auch bereits bestehender Anforderungen muss künftig durch unabhängige Tests geprüft werden[4].

Eine Weiterentwicklung und der weitere Betrieb von Video-Ident ohne Kenntnis der notwendigen Gegenmaßnahmen, ohne sichere Zulassungsprozesse und belegtes Vertrauensniveau ist insbesondere im Gesundheitswesen nicht zu verantworten. Prinzipien wie „Fail fast, fail often“ dürfen im Kontext von digitalen Identitäten keine Anwendung finden (Wittmann, 2021).

[4] So fordert das BSI zwar die „Manipulierbarkeit des verwendeten ID-Dokuments […] zu betrachten und die erreichbare FAR […] zu bestimmen“, verzichtet für Einstufung in substantielles Vertrauensniveau jedoch auf „unabhängige Tests“ (Bundesamt für Sicherheit in der Informationstechnik, 2021).

Literaturverzeichnis

Bay, H., Tuytelaars, T., & Van Gool, L. (2006). SURF: Speeded Up Robust Features. *Proceedings of the 9th European Conference on Computer Vision.* Springer Verlag.

BILD am SONNTAG. (3. Februar 2019). Sicherheitsbehörde warnt vor neuem Identitätsbetrug im Internet. *BILD am SONNTAG*. Von https://www.bild.de/bild-plus/politik/inland/politik-inland/abzockgefahr-zeigen-sie-nie-ihren-ausweis-im-internet-59915814.bild.html abgerufen

bitkom. (Mai 2018). Stellungnahme: Videoidentifikation als national anerkannte Identifikationsmethode – ein notwendiger Schritt für die Digitalisierung und den europäischen Binnenmarkt. Von https://www.bitkom.org/sites/main/files/file/import/20180712-Bitkom-Position-zum-Videoidentverfahren-als-national-anerkannte-Identifikationsmethode.pdf abgerufen

bitkom; vatm. (15. Juni 2021). Stellungnahme; Anhörung zur Neugestaltung der Verfügung gemäß § 111 Absatz 1 Satz 4 Telekommunikationsgesetz. Von https://www.bitkom.org/sites/default/files/2021-06/bitkom-vatm_verbande-stellungnahme_verifizierung-111-tkg.pdf abgerufen

Bradski, G. (2000). The OpenCV Library. *Dr. Dobb's Journal of Software Tools*, S. 120; 122-125.

Bundesamt für Sicherheit in der Informationstechnik. (17. Mai 2017). Differenzierte Vertrauensniveaus für die Identitätsprüfung; Zwischen Sicherheit und Nutzerfreundlichkeit. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/15ter/Vortraege_17-05-2017/ThomasSchnattinger.pdf abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (18. September 2018). Verifikation der Identität – Verwendung des nPA. Von https://www.teletrust.de/fileadmin/docs/veranstaltungen/Signaturtag_2018/11_Informationstag_Elektronische-Signatur-und-Vertrauensdienste_Frank-BSI.pdf abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (26. August 2019). Technical Guideline TR-03159 Mobile Identities Part 1: Security Requirements for eIDAS LoA “substantial”; Version 1.0 Draft 2. Von https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-1.pdf abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (7. Mai 2019). Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government; Teil 1: Vertrauensniveaus und Mechanismen; Version 1.1.1.

Bundesamt für Sicherheit in der Informationstechnik. (28. 12 2021). Anforderungskatalog zur Prüfung von Identifikationsverfahren gemäß TR-03147 in Version 1.0.6; Version 1.0.0; 28.12.2021. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR-03147-1_Anforderungen.pdf abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (28. Dezember 2021). Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen, Version 1.0.6. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR03147.pdf abgerufen

Bundesanstalt für Finanzdienstleistungsaufsicht. (5. März 2014). Rundschreiben 1/2014 (GW) - Verdachtsmeldung nach §§ 11, 14 GwG und anderes. Von

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm.html abgerufen

Bundesanstalt für Finanzdienstleistungsaufsicht. (10. April 2017). Rundschreiben 3/2017 (GW) - Videoidentifizierungsverfahren. Von https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html abgerufen

Bundesanstalt für Finanzdienstleistungsaufsicht. (9. Mai 2022). Ergebnis der Evaluierung des Videoidentifizierungsverfahrens i. S. d. Rundschreibens 3/2017 (GW). Von https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Auslegungsentscheidung/A/ae_videoident_rs_3_2017.html abgerufen

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (17. Juni 2015). Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. (8. Mai 2019). Tätigkeitsbericht 2017 – 2018; 27. Tätigkeitsbericht. Von https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/27TB_17_18.pdf abgerufen

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. (25. März 2021). Tätigkeitsbericht 2020; 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit. Von https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/29TB_20.pdf abgerufen

Bundesministerium des Innern, für Bau und Heimat. (August 2021). Cybersicherheitsstrategie für Deutschland 2021. Von https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf abgerufen

Bundesministerium des Innern, für Bau und Heimat. (August 2021). Der Personalausweis. (f. B. Bundesministerium des Innern, Hrsg.)

Bundesministerium für Wirtschaft und Klimaschutz. (19. Mai 2020). *Nect Robo-Ident: Die Zukunft der Fernidentifizierung für Krankenkassen, Versicherungen und Banken.* Von BMWK.de: https://www.bmwk.de/Redaktion/DE/Wettbewerb/Fragmente/innovationspreis-reallabore-nect-robo-ident.html abgerufen

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. (13. Juni 2018). Mitteilungen, Qualifizierte elektronische Signatur, Teil A, Mitteilungen der Bundesnetzagentur. *Amtsblatt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, S. 924-931.

Bundesregierung. (9. Juli 2019). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Bettina Stark-Watzinger, Christian Dürr, Daniela Kluckert, weiterer Abgeordneter und der Fraktion der FDP; Video-Ident-Verfahren bei Finanzdienstleistungen; Drucksache 19/11443. Von https://dserver.bundestag.de/btd/19/114/1911443.pdf abgerufen

Burt, C. (4. Mai 2022). *Workshop showcases EU progress on remote identity proofing, but fragmentation persists*. Von BiometricUpdate.com: https://www.biometricupdate.com/202205/workshop-showcases-eu-progress-on-remote-identity-proofing-but-fragmentation-persists abgerufen

Common Criteria. (April 2017). Common Methodology for Information Technology Security Evaluation; Evaluation methodology; Version 3.1; Revision 5. Von https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf abgerufen

Deutscher Bundestag. (13. Januar 2021). Stenografischer Bericht; 203. Sitzung; Plenarprotokoll 19/2013. 25593.

ETSI. (Juli 2021). ETSI TS 119 461 V1.1.1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. Von https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf abgerufen

Europäische Kommission. (Dezember 2019). Report on existing remote on-boarding solutions in the banking sector; Assessment of Risks and Associated Mitigating Controls, Including Interoperability of the Remote Solutions. Von https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf abgerufen

European Union Agency for Cybersecurity. (20. Januar 2022). Remote Identity Proofing: Attacks & Countermeasures. Von https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures abgerufen

gematik GmbH. (19. Januar 2019). Festlegung der gematik bzgl. der Umsetzung des § 336 Absatz 5 SGB V bei der Herausgabe der eGK. Von https://fachportal.gematik.de/fileadmin/Fachportal/Krankenversicherung/Stellungnahme_eGK.pdf abgerufen

Herpers, R., Scherfgen, D., Jato, O., Millberg, J., & Hinkenjann, A. (3. Mai 2022). Deep Faked Video Identity Manipulations. Von https://www.enisa.europa.eu/events/enisa-etsi-joint-workshop-on-remote-identity-proofing/workshop-presentations/1-1-rainer-herpers-deep-fake-video-identity-manipulations.pdf abgerufen

Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science, 332*(6025), S. 60-65. doi:10.1126/science.1200970

IDnow GmbH. (18. September 2018). Informationstag "Elektronische Signatur und Vertrauensdienste"; Gemeinsame Veranstaltung von TeleTrusT und VOI; Technologien für eine sichere Identifikation. Von https://www.teletrust.de/fileadmin/docs/veranstaltungen/Signaturtag_2018/10_Informationstag_Elektronische-Signatur-und-Vertrauensdienste_Sittek_IDNow.pdf abgerufen

IDnow GmbH. (24. September 2019). TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste" 2019 Bundesverband IT-Sicherheit e.V. (TeleTrusT); Quo vadis Vertrauensdienste; Aktuelle technische und regulatorische Trends bei der Identifikation.

Kriegman, D. (2007). *Explanation of Homography Estimation.* Von https://cseweb.ucsd.edu//classes/wi07/cse252a/homography_estimation/homography_estimation.pdf abgerufen

Nect GmbH. (13. Juni 2019). Nect Selfie-Ident im Kundenportal „Meine R+V“. Von https://www.bitkom.org/sites/default/files/2019-06/kundenfreundliche_identitatsfeststellung_-_ein_digitales_erfolgsmodell.pdf abgerufen

S. Garrido-Jurado, R. M.-S.-C.-J. (Juni 2014). Automatic generation and detection of highly reliable fiducial markers under occlusion. *Pattern Recognition, 47*(6), S. 2280-2292. doi:https://doi.org/10.1016/j.patcog.2014.01.005

Sensity B.V. (13. 10 2021). ID Verification Spoofing. Von https://www.youtube.com/watch?v=SU9K1LsgX7c abgerufen

Sensity B.V. (Mai 2022). Deepfakes vs Biometric KYC Verification. Von https://sensity.ai/blog/deepfake-detection/deepfakes-vs-kyc-biometric-verification/ abgerufen

Sensity B.V. (4. Juni 2022). The Deepfake Offensive Toolkit. Von https://github.com/sensity-ai/dot abgerufen

Techniker Krankenkasse. (15. Juni 2022). *Was ist Nect Ident?* Von tk.de: https://www.tk.de/techniker/leistungen-und-mitgliedschaft/informationen-versicherte/was-ist-meine-tk/weitere-haeufige-fragen-meine-tk/selfie-video-ident-verfahren/was-ist-nect-ident-2097866 abgerufen

TÜV TRUST IT. (3. Mai 2022). ENISA & ETSI Workshop Remote Identity Proofing; The Challenge of Auditing Deep Learning Based Identity Proofing Processes. Von https://www.enisa.europa.eu/events/enisa-etsi-joint-workshop-on-remote-identity-proofing/workshop-presentations/3-3-tuv-austria-the-challenge-of-auditing-deep-learning-based-identity-proofing-processes.pdf abgerufen

Weyrich, T., Lawrence, J., P. A. Lensch, H., Rusinkiewicz, S., & Zickler, T. (2009). *Principles of Appearance Acquisition and Representation.* now.

Wirtschaftsforum der SPD e.V. (2020. Januar 2019). Arbeitssitzung zur Zukunft des Video-Ident-Verfahrens. Von https://www.spd-wirtschaftsforum.de/veranstaltung/zukunft-video-ident/ abgerufen

Wittmann, L. (29. September 2021). Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen. Von https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0 abgerufen

Anhang

Zeitleiste des Video-Idents

Januar 2013	Idnow GmbH stellt Antrag auf Video-Ident-Patent EP2948891B1.
August 2013	WebID Solutions GmbH stellt Antrag auf Video-Ident-Patent US11017223B2.
März 2014	Die Bafin bewertet Video-Ident als GWG-tauglich.
Mai 2015	Deutsche Post DHL Group führt POSTIDENT VIDEO ein.
Juni 2015	Die BfDI veröffentlicht im 25. Tätigkeitsbericht zum Datenschutz 2013 – 2014: „Ein solches [Video-Ident-]Verfahren verstößt nach meiner Auffassung nicht nur gegen das GwG, sondern birgt auch erhebliche datenschutzrechtliche Risiken. Denn Sinn und Zweck einer persönlichen Anwesenheit besteht darin, zweifelsfrei die Übereinstimmung von personenbezogenen Ausweisdaten und anwesender Person sowie Echtheit des Ausweises überprüfen zu können. Ob die Zuverlässigkeit der „Inaugenscheinnahme“ einer Person und ihres Ausweises mittels Videotechnik dem unmittelbaren persönlichen Kontakt gleichgestellt werden kann, erscheint mir mehr als fraglich. Über eine Videoverbindung können beispielsweise Sicherheitsmerkmale des Ausweises wie Hologramme nicht eindeutig als echt erkannt werden. Auch andere Manipulationen am Ausweis sind nicht ohne weiteres so offensichtlich wie bei einer tatsächlichen Inaugenscheinnahme.“
Oktober 2016	WebID GmbH beschreibt Risiko durch technische Manipulation (Maskierung) des übertragenen Videobildes eines Dokuments oder eines Gesichts: „When examining an object, for example a document, in particular a badge, or, for example, a face in a video call, there is a risk that the object to be checked will be "masked" by technical manipulation of the transmitted video image.“
September 2017	Das BSI stellt Ergebnisse der „Vito“-Studie u. a. auf dem EDVGT 2017 vor, darunter erfolgreiche „Manipulationen und Simulationen des Ausweisdokuments auf videobearbeitungstechnischer Ebene“ unter Einsatz von „Standardkomponenten“.
Dezember 2017	SURFcontext stellt fest: „Real time video morphing technology is advancing rapidly and allows the user to pretend to be someone else or to alter the identity document. The German Federal Office for Information Security did some experiments with morphing technology and concluded that video is not optimal for identity verification purposes.“
September 2018	Das BSI sieht moderates Angriffspotential: „Optische Sicherheitsmerkmale können nicht sicher digitalisiert werden“.
September 2018	Das BSI warnt im Lagebericht 2018 vor „Identitätsmissbrauch durch Fernidentifizierungsverfahren“: „Ein mit dem Smartphone aufgenommenes Videobild des Nutzers und seines Ausweises ist in Bezug auf Eindeutigkeit

und Sicherheit nicht vergleichbar mit einer Identifizierung bei physischer Anwesenheit."

September 2018 Sicherheitsexperten der NTT Group sehen die „Manipulation von Authentifizierungsverfahren" mittels „Umgehung von kamera- oder audiobasierten Authentifizierungsmechanismen durch manipulierte Bilder und Videos".

November 2018 Die Bundesnetzagentur hat nach Anhörung der betroffenen Kreise und im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik die erstmalige Verfügung i.S.d. § 11 Absatz 1 VDG im Amtsblatt 11/2018 vom 13.06.2018 (Mitteilung Nr. 208) veröffentlicht.

Januar 2019 Die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) schreibt im Jahresbericht 2018: „Eine Ausnahme stellt die hohe Anzahl von gemeldeten Transaktionen dar, die Frankreich sowohl zum Ursprungs- als auch zum Bestimmungsland haben, jedoch über ein deutsches Konto abgewickelt wurden. Hier ist eine Häufung von in betrügerischer Absicht eröffneten Konten bei deutschen Internetbanken festzustellen, bei denen eine Identifizierung ohne physische Anwesenheit, beispielsweise über ein Video-Ident-Verfahren, möglich ist."

Februar 2019 Das BSI „warnt vor Sicherheitsrisiken beim sogenannten Video-Ident-Verfahren" und rät „Video-Ident nicht zu nutzen". Sicherheitsvorkehrungen bei Video-Ident könnten mithilfe von Bildmanipulationen sowie falschen oder gestohlenen persönlichen Daten ausgetrickst werden.

Mai 2019 Der BfDI schreibt im Tätigkeitsbericht zum Datenschutz 2017 – 2018: „Die Videoidentifizierung weist nicht das gleiche Sicherheitsniveau auf, wie die Identifizierung unter Anwesenden. Eine Dokumentenprüfung ist nach dem heutigen Stand der Technik in einem Videokanal nicht vollumfänglich möglich. Daher kann bei einer Videoidentifizierung noch schlechter als bei der Identifizierung vor Ort unterschieden werden, ob ein Ausweisdokument echt ist oder eine Fälschung vorliegt […]. Da die Integrität der zur Identifizierung herangezogenen Daten maßgeblich für jedwede sichere Identifizierungsmethode ist, bei der Videoidentifizierung aber nicht erfüllt werden kann, lehne ich diese Identifizierungsmethode ab."

August 2019 Das BSI kennt „derzeit keine zuverlässigen Methoden zur Erkennung von Präsentationsangriffen" bei aus der Ferne verifizierten biometrische Daten". BSI TR-03159 „Remotely verified biometrics are not supported by the Technical Guideline, since there are currently no reliable methods for presentation attack detection available in this scenario."

Juli 2019 „Der Bundesregierung sind bislang keine Betrugsfälle beim sogenannten Video-Ident-Verfahren bekannt, bei denen der Video-Stream mittels eines Hackerangriffs manipuliert worden ist." Gleichsam erhält sie „keine Meldungen der Betreiber von Video-Ident-Verfahren über Betrugsversuche."

Dezember 2019	Der Bundesgerichtshof (BGH) begründet mit Beschluss 4 Ars 14/19 die Notwendigkeit der Vorlage des Original-ID-Dokuments gegenüber der elektronischen Übersendung eines Bildes: „Auch der Rechtsverkehr verlangt zur Identifizierung einer Person jedenfalls in denjenigen Fällen, in denen der Identität der Person für das Rechtsgeschäft eine herausgehobene Bedeutung zukommt, unverändert die Vorlage der Urschrift des Ausweispapiers. Dies zeigt sich insbesondere bei notariell zu beurkundenden Rechtsgeschäften sowie Rechtsgeschäften im Anwendungsbereich des Geldwäschegesetzes.“
Januar 2020	Die FIU schreibt im Jahresbericht 2019: „Zudem wurden wie bereits im Jahr 2018 auffällig viele Transaktionen gemeldet, bei denen sowohl das Herkunfts- als auch das Bestimmungsland Frankreich ist. In diesen Fällen ist zudem eine Häufung von in betrügerischer Absicht eröffneten Konten bei deutschen Internetbanken festzustellen, bei denen eine Identifizierung ohne physische Anwesenheit, beispielsweise über ein Video-Ident-Verfahren, möglich ist.“
Januar 2021	Die FIU schreibt im Jahresbericht 2020: „Das Video-Ident-Verfahren bietet ein erhebliches Missbrauchspotential.“
Januar 2021	Das BSI empfiehlt Video-Ident „wegen des hohen Schutzbedarfs von Gesundheitsdaten für den benannten Einsatzzweck grundsätzlich als nicht geeignet anzusehen“
Januar 2021	Die Bundesregierung schreibt: „Weiterhin ist die nachträgliche Identifikation beispielsweise unter Nutzung eines Video-Ident-Verfahrens, einer Postfiliale oder der eID-Funktion des elektronischen Personalausweises möglich. Nach Kenntnis der Bundesregierung können auch Online-Ident-Verfahren die Voraussetzungen für eine solche sichere Identifizierung nach § 336 Fünftes Buch Sozialgesetzbuch (SGB V) erfüllen.“
Januar 2021	Die gematik lässt Video-Ident zu: „Bis auf Weiteres ist die Nutzung des VideoIdent-Verfahrens ohne Operator (vollautomatisierte VideoIdent-Verfahren ohne Prüfung durch einen Mitarbeiter) zur nachträglichen Identifikation des Versicherten zugelassen.“
März 2021	Der BfDI veröffentlicht im Tätigkeitsbericht 2020 eine „Grundsatzentscheidung des BfDI“: „Videoidentifizierungsverfahren sind risikobehaftet. Wo ein sehr hohes Vertrauensniveau erreicht werden muss, sind sie datenschutzrechtlich sogar unzulässig.“ Dies gilt in Bereichen „in denen die Identifizierung ein sehr hohes Vertrauensniveau erfüllen muss“ wie beispielsweise „zum Schutz besonders schutzbedürftiger Kategorien von personenbezogenen Daten nach Artikel 9 DSGVO, wie etwa im Gesundheitswesen“.
April 2021	Die BNetzA veröffentlicht im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und nach Anhörung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am

01.04.2021 eine neue Verfügung zu Videoidentifizierung mit automatisiertem Verfahren.

Juni 2021 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität:
Die Bestimmungen über den Einsatz von Fernidentifizierungsmitteln wurden „harmonisiert und präzisiert". Die Identifizierung nach Artikel 24 Absatz 1 Buchstabe d) muss nun keine „gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit" mehr bieten.

Juni 2022 Die BaFin veröffentlicht das „Ergebnis der Evaluierung des Videoidentifizierungsverfahrens i. S. d. Rundschreibens 3/2017 (GW)": „Das Videoidentifizierungsverfahren wird als Brückentechnologie weiter fortgeführt."