.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Daubner, Franz/Strobl, Bernhard

Modentity. Smartphone-basierte hochmobile Dokumenten- und Identitätsverifikation für die Personenkontrolle der Zukunft

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3/2017), 41-52.

doi: 10.7396/2017_3_D

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Daubner, Franz/Strobl, Bernhard (2017). Modentity. Smartphone-basierte hochmobile Dokumenten- und Identitätsverifikation für die Personenkontrolle der Zukunft, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 41-52, Online: http://dx.doi.org/10.7396/2017_3_D.

Hinweis: Die gedruckte Ausgabe des Artikels ist in der Print-Version des SIAK-Journals im Verlag NWV (http://nwv.at) erschienen.

Online publiziert: 4/2018

Modentity

Smartphone-basierte hochmobile Dokumenten- und Identitätsverifikation für die Personenkontrolle der Zukunft

Eine effiziente und hoch verlässliche Dokumenten- und Identitätsverifikation für die Personenkontrolle im Rahmen der Grenzsicherung ist in Zeiten höchster Personenmobilität, aber auch vor dem Hintergrund der anhaltenden Flüchtlingsströme, eine der aktuell größten gesellschaftlichen Herausforderungen. Sichere Grenzen, auch im Sinne des Schutzes der EU-Außengrenzen des Schengenraumes, bestimmen in hohem Maße das Sicherheitsgefühl der Bevölkerung. In Österreich misst rund ein Drittel der hier lebenden Menschen ausreichend gesicherten Grenzen eine wichtige Rolle für die nationale Sicherheit bei. Personenkontrollen finden aber nicht nur an den tatsächlichen Grenzübertritts- bzw. Einreiselokationen wie auf Flughäfen statt, sondern werden auch im Rahmen von behördlich durchgeführten Ausgleichsmaßnahmen im Hinterland durchgeführt. Neben diesem breiteren Ansatz der Personenkontrolle und Grenzsicherung wird der Erfolg der Bundespolizeibehörden und anderer als „first responder" tätiger Einsatzkräfte vor allem durch den Einsatz laufend verbesserter technologischer Methoden zur Dokumenten- und Identitätsverifikation bestimmt. Die Zielsetzungen für zukunftstaugliche Verfahren und Tools fordern daher objektiv und rasch durchführbare Überprüfungen auf Basis heute üblicher biometrischer Verfahren. Nur mit ihnen kann ein hoher Qualitätsgrad erreicht werden, mit dem die Einsatzkräfte der Exekutive ihre Aufgabenstellungen in der Personenfahndung, bei der Bekämpfung und Vermeidung illegaler Einwanderung bzw. von illegalem Aufenthalt sowie von damit verbundener Kriminalität und Terrorismusakten erfolgreich bewältigen können.

FRANZ DAUBNER,
Modentity Projektleiter im Center for Digital Safety & Security am AIT Austrian Institute of Technology.

BERNHARD STROBL,
Thematic Coordinator im Center for Digital Safety & Security am AIT Austrian Institute of Technology.

1. KIRAS-FORSCHUNGSPROJEKT „MODENTITY"

Zwischen 1. November 2014 und 30. November 2016 wurde unter Konsortialführung des AIT Austrian Institute of Technology, Department Digital Safety & Security (heute: Center for Digital Safety & Security), in Zusammenarbeit mit dem Bedarfsträger Bundesministerium für Inneres (BMI), der Österreichischen Staatsdruckerei GmbH (Hersteller der österreichischen Reisepässe), der rubicon IT GmbH sowie dem Institut für empirische Sozialforschung (IFES) GmbH und der IFES Feld GmbH das KIRAS-Forschungsprojekt (Österreichisches Sicherheitsforschungsprogramm) „Modentity" zur weiteren Verbesserung der Dokumenten- und Identitätsverifikation für Personenkontrollen der Zukunft durchgeführt und zu einem erfolgreichen Abschluss gebracht.

Bei dem Forschungsprojekt ging es, ausgehend von den Anforderungen des Bedarfsträgers BMI, die sowohl durch

Experteninterviews als auch durch Vor-Ort-Analysen mit (Grenzschutz-)Beamten im Rahmen der von ihnen durchgeführten Ausgleichsmaßnahmen sowie in einem zusammenfassenden Workshop erhoben wurden, zuerst um die Erfassung der typischen Abläufe einer Personenkontrolle für fünf unterschiedliche Use Cases: Kontrolle in Nachtzügen, Personalkontrolle auf Frachtschiffen, Schwerpunktkontrollen Autobahn, tägliche Polizeiarbeit auf Polizeiinspektionen und Vorfeldkontrolle auf Flughäfen (Ankunfts- und Abflughallen). In einem Anforderungsdokument wurden die 47 ermittelten Anforderungen in funktionale und nicht-funktionale Anforderungen aufgeteilt und gemeinsam mit dem Bedarfsträger priorisiert.

Diese Bedarfserhebung bildete im Projekt den Ausgangspunkt für das Gesamtanforderungsprofil (Pflichtenheft) einer zu konzipierenden mobilen Plattform für die Nutzung von Smartphones des Betriebssystems Android zur Dokumenten- und Identitätsverifikation bei Personenkontrollen in den zuvor geschilderten Szenarien.

Stark pointiert dargestellt muss eine mobile Grenzkontrolllösung die funktionalen Anforderungen der Erfassung und Überprüfung von Dokumenten (Reisepässe bzw. elektronische ICAO[1]-konforme ID-Ausweise wie Personalausweise oder Aufenthaltstitel) durch Auslesen des kontaktlosen Chips, die Erfassung, Qualitätsbewertung und Verifikation biometrischer Merkmale, wie Fingerabdrücke und Gesichtsbilder mit entsprechender Kontrolltiefe und das Auslesen von OCR (Optical Character Recognition), also der Dokumentendaten aus der MRZ (Machine-Readable Zone) ermöglichen und darüber hinaus die Erfüllung der nicht-funktionalen Anforderungen in Bezug auf Zuverlässigkeit, Handhabung (beste Usability) und Look and Feel, Leistung und Effizienz (z.B. Akkuleistung für mindestens zwölf Stunden/bis zu 600 Kontrollen im Szenario Autobahn) und höchste Geräte- und Applikationssicherheit gewährleisten.

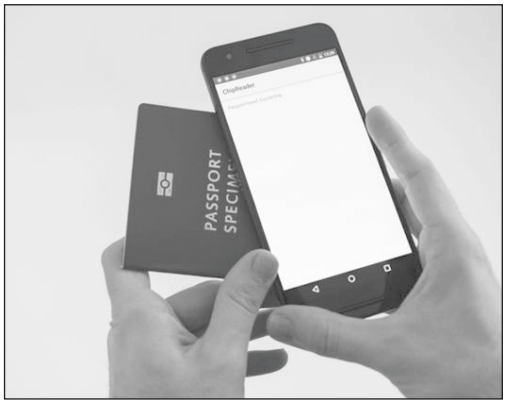
Von ganz entscheidender Bedeutung für die Effizienz der Kontrollroutine sind auch die mobile, quasi unterbrechungslose Datenanbindung und die hohe Funktionalität der Dateninterfaces zur weitgehend automatisierten Abfrage von nationalen und internationalen Hintergrundsystemen/Datenbanken wie des VISA-Informationssystems (VIS) bzw. der Sachen- und Personenfahndung, des Erweiterten Schengener Informationssystems (SIS II), des Elektronischen Kriminalpolizeilichen Informationssystems (EKIS), des Fremdenpolizeilichen Informationssystems (FIS) und der Integrierten Fremdenapplikation (IFA) auf Basis der Reisedokumente (MRZ), der Dokumentennummern (z.B. bei Führerscheinen) bzw. der Kfz-Kennzeichen.

Wie bei KIRAS-Forschungsprojekten zwingend erforderlich, wurden auch im Projekt „Modentity“ die gesellschaftlichen, ethischen, sozialen und auch die Umweltaspekte durch eine begleitende, von IFES durchgeführte GSK-Studie, berücksichtigt, deren Ergebnisse laufend in den technologischen Entwicklungsprozess der mobilen Plattform zur Erhöhung der Grenzkontrollsicherheit und des Sicherheitsgefühls der Bevölkerung mit einbezogen wurden. Die Ausräumung, insbesondere ethischer Bedenken gegen die Erfassung und Bearbeitung biometrischer Merkmale durch die Sicherheitsbehörden, erfolgte im Projekt auf Basis breiter Aufklärungsarbeit in direkten Interaktionen mit der Bevölkerung.

Die Anforderungen an höchste Datensicherheit und konsequenten Datenschutz wurden bei Modentity von Anfang an per Design (Privacy by Design) berücksichtigt. Die Einhaltung aller europäischen und österreichischen Normen und Gesetze wurde

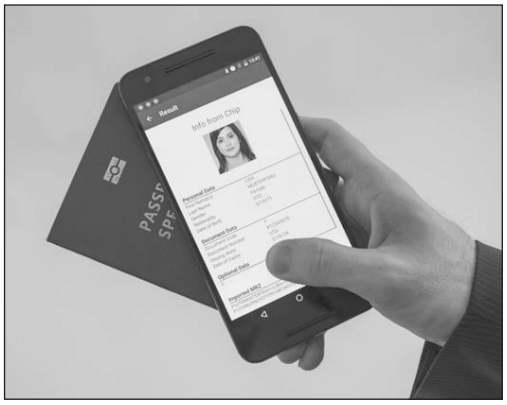
zudem durch Abstimmung mit der Datenschutzkommission überprüft. Ein ergänzend eingeholtes Rechtsgutachten bescheinigte den Projektverantwortlichen, dass der Anwendung des Modentity-Konzeptes im Rahmen von Grenzkontrollaktivitäten aus GSK-Perspektive nichts im Wege steht und bestätigte damit das Resümee der IFES-Studie über eine erstaunlich hohe Akzeptanz dieses modernen Technologieeinsatzes zur Verbesserung des Grenzschutzes auch im Sinne der verbesserten Prävention gegen illegale Einwanderung in der Bevölkerung.

Quelle: Modentity Konsortium



Durch einfaches „Anhalten" des elektronischen Reisedokumentes wird der Chipinhalt gelesen und verifiziert

Quelle: Modentity Konsortium



Anzeige der Daten des Passchips

2. INNOVATIONSGEHALT DES PROJEKTES „MODENTITY"

Die derzeit verwendeten Systeme der Dokumenten- und Identitätsverifikation können zwar an stationären Grenzkontrollstandorten ihre Funktionalität ausspielen, für den mobilen Einsatz, wie er bei fremden- und kriminalpolizeilichen Ausgleichsmaßnahmen abseits der zentralen Landeseintrittslokationen (Land-Grenzübergänge, Flughäfen) erforderlich ist, sind sie jedoch nur bedingt geeignet. Laptops mit angeschlossenen Zusatzgeräten, wie Vollflächen-Pass-Scannern und im Idealfall Fingerabdruck-Erfassungsgeräten, sind für Kontrollszenarien wie sie für die fünf in Modentity definierten Use-Cases benötigt werden, alleine schon auf Grund ihrer Sperrigkeit ungeeignet. Auch die massiven Ablaufbehinderungen durch kurzweiligen Ausfall der mobilen Datenverbindung (z.B. in Eisenbahntunnels) erfordern neue, innovative Ansätze der Dokumenten- und Identitätsverifikation mit kleinen Geräten von bester Usability.

Um die beschriebenen Limitierungen in der mobilen Grenzkontrolle zu überwinden, wurden im Projekt „Modentity" vier konkrete Innovationsleistungen adressiert:

a) Die Dokumentenverifikation soll mit einem handelsüblichen Smartphone unter Verwendung der integrierten Kamera und mittels eines RFID[2]-Readers möglich sein.
b) Die Identitätsverifikation soll mit einem handelsüblichen Smartphone durch Verwendung der Kamera und von Fingerabdrucksensoren erfolgen können.
c) Weitere für den Kontrollprozess wichtige, drahtlose Sensoren müssen als Module integrierbar sein.
d) Es müssen robuste und ausfallsichere mobile Kommunikationsverbindungen zu allen für den erkennungsdienstlichen Workflow wesentlichen Datenbanken zur Verfügung stehen.

Für die Umsetzung dieser Innovationsziele wurden im Projekt alle relevanten Faktoren, die nachfolgend beschrieben werden, erforscht und die Einsatztaug-

lichkeit des technologischen Konzepts, verstanden als die Summe der erforderlichen Architekturen, Prozesse und Applikationen, in einem „proof-of-concept" demonstriert.

3. KERNELEMENTE DER „MODENTITY"-LÖSUNG

Das in Modentity entwickelte Gesamtsystem der Dokumenten- und Identitätsprüfung für den mobilen Einsatz bei Personenkontrollen im Zuge von Ausgleichsmaßnahmen beruht im Kern auf einer App, die als Modulsystem aufgebaut ist. Jede einzelne Funktionalität zum Einlesen von Daten (Lesen des Reisepasses, Lesen des Fingerabdrucks, Datenbankabfragen) ist als eigenes Modul ausgeführt. Beim entwickelten System können einfach erforderliche Module hinzugefügt bzw. nicht mehr benötigte Module entfernt werden, ohne die Core-App ändern zu müssen.

Um eine Person hinsichtlich ihrer Identität eindeutig überprüfen zu können, sind bei der Grenzkontrolle im Grunde drei Kernroutinen erforderlich, die vom modularen Gesamtsystem technologisch abgedeckt werden müssen.

a) Optisches und elektronisches Auslesen des vorgelegten Identitätsdokuments und Verifizierung dieser Daten im Sinne der Echtheitsprüfung.
b) Aufnahme biometrischer Merkmale einer Person und real-time Abgleich mit den gespeicherten Merkmalen im vorgelegten Identitätsdokument. Mit diesem zweiten Prozessschritt wird die Verbindung zwischen Person und Identität hergestellt. Nur wenn die biometrischen Daten übereinstimmen, kann die Identität aus dem Dokument eindeutig der überprüften Person zugeordnet werden.
c) Abgleich der ermittelten Identität gegen relevante Datenbanken.

Um diese Prozessschritte hoch automatisiert bewältigen zu können, werden an eine mobile Lösung mittels Smartphone hohe Anforderungen bezüglich Soft- und Hardware gestellt. So werden für das Auslesen der Chipdaten aus den Dokumenten mit kontaktlosen bzw. kontaktbehafteten Chips, für das optische Auslesen von gedruckten Daten aus dem Dokument mittels Optical Character Recognition (OCR) und das Überprüfen der optisch ausgelesenen Daten bzw. deren Vergleich mit den elektronisch ausgelesenen Daten mittels Optical Character Verification (OCV) bzw. die Prüfung von Eigenschaften und Sicherheitsmerkmalen des Dokuments zur Bestimmung seiner Echtheit (Optical Character Authentication) sowie zum Überprüfen biometrischer Eigenschaften durch Zuordnung von im Dokument gespeicherten Informationen mit aktuell vermessenen Körpereigenschaften (Vorort-Scanns) des Dokumentenbesitzers (z.B. Fingerabdrucks- oder Gesichtsverifikation) unterschiedlichste funktionale Softwarelösungen benötigt.

Hardware-seitig sind für die Dokumentenüberprüfung und Identitätsfeststellung unterschiedlichste Sensoren und Bilderfassungsgeräte sowie RFID-Reader für die Prüfung von Dokumenten mit kontaktlosen Chips erforderlich. Manche dieser Sensoren sind in High-End-Smartphones der letzten Generation bereits integriert,

Quelle: Modentity Konsortium

Durch einfaches Abfilmen der „visible page" des Reisedokuments kann die MRZ gelesen und verifiziert werden

Quelle: Modentity Konsortium

Anzeige der bereits digital erfassten Passinhalte

manche müssen durch externe Sensoren ersetzt werden.

4. HAUPTINNOVATION: FINGERABDRUCKAUFZEICHNUNG MITTELS SMARTPHONE-KAMERA

Im Projekt „Modentity" wurden alternative Leseverfahren, wie die kamerabasierte Dokumentenauthentifizierung, die mobile Gesichtserkennung, die kamerabasierte Fingerprintverifizierung und das geräteeigene Auslesen von Fingerabdrücken, erforscht.

Das Highlight im Bereich Technologieinnovation gelang dem Projektteam unter Führung des AIT mit der Entwicklung einer Software zur kontaktlosen Fingerabdruckaufzeichnung mittels der Smartphonekamera. Damit aufgenommene, so genannte „touchless fingerprints", stellen die Verarbeitungsalgorithmen zur Extraktion und Aufbereitung von Fingerabdruckbildern vor neue Herausforderungen, weil z.B. einerseits keine totale Kontrolle des Aufnahmeprozesses in Bezug auf die Distanz zum Sensor oder auch die Abschirmung von Licht gewährleistet werden kann, andererseits aber im Kontext von behördlichen Identitäts-Verifizierungsprozessen eine hohe Erwartungserhaltung hinsichtlich einer ausreichenden Qualität im Vergleich mit herkömmlichen berührungsbasierten Geräten (FTIR Sensor, Kapazitiver Sensor) oder mit kostspieligen dedizierten Geräten (wie z.B. dem Morpho Wave Sensor mit Kosten um die 5.000 €) vorliegt.

Auf dem Weg zur Prototypenentwicklung mussten vor allem Herausforderungen bezüglich des Aufnahme-Hardware-Setups, Problemstellungen in Bezug auf die Distanzmessung, der Segmentierung (Separierung der Finger von Hintergrundinformationen und Positions- und Lagebestimmung), der Bildverbesserungsverfahren, der Merkmalsextraktion und von Vergleichsalgorithmen gelöst werden.

Das neuartige Verfahren der kontaktlosen Aufnahme von Fingerabdrücken, welches insbesondere bei Reisenden aus dem asiatischen Raum kulturell bedingt auf große Resonanz stoßen dürfte, erlaubt die Erfassung aller zehn Finger in drei Schritten (vier Finger links, vier Finger rechts, Daumen). Das Auslesen über ein externes Gerät über Bluetooth ist ebenfalls möglich.

Da der Abgleich von Fingerabdrücken zentraler Bestandteil des Identitäts-Verifikationsprozesses ist und in den derzeit verfügbaren Smartphones Fingerabdrucksensoren äußerst selten integriert sind, war es erklärtes Ziel des Projektes, diese Funktionalität auch mit Smartphones zur Verfügung zu stellen, die keinen integrierten Fingerabdrucksensor haben.

Quelle: Modentity Konsortium

Mögliche externe Sensorik zur erweiterten Erfassung

4.1 Vorgehen

Um eine erfolgreiche Abwicklung der Biometrie-Entwicklung zu gewährleisten, wurde ein agiler Ansatz gewählt, der aus folgenden Teilaufgaben bestand:

- Festlegung Hardware-Setup zur Aufnahme
  - Autofokus versus fixer Fokus (mit Bewegung der Hand, um scharfe Aufnahmen zu gewährleisten),
  - Freie 4-Finger „Fingerphoto" Aufnahme,
  - Erstellung von Test-Aufnahmen zur Ermittlung der Tiefenschärfe (DoF, Depth of Field) und Auflösung (DPI),
  - Untersuchung der Möglichkeit Aufnahme 4-Finger vs. 1-Finger.
- Entwicklung eines Prototypen zur Bildsegmentierung
  - Untersuchung Skin-Color basierte Verfahren versus Kanten-basierte Verfahren.
- Einbindung der NBIS-Software und Aufbauen einer Bildverarbeitungskette
  - C++/Visual-Studio Projekt, nur OpenCV als externe Abhängigkeit (+boost, fftw für Commandline-Tools),
  - Kontrolle der gesamten Bildverarbeitungskette (Vorverarbeitung, Merkmalsextraktion, Vergleich, QA).
- Aufnahme eines Testdatensets und Auswertung

Die Herausforderung des zu entwickelnden Verfahrens liegt in der geeigneten Aufbereitung der Abdrücke, sodass Charakteristika von Touch-basierten Sensoren (500 dpi-Aufnahme, integrierte QA, „Ridges" [Papillarleisten]: schwarz „Valleys": weiß und ideal: hoher Ridge/Valley Kontrast, klare Verzweigungen, gute Auflage) erhalten werden.

4.2 Distanzmessung

In einem ersten Versuchsaufbau wurden die Aufnahmebedingungen unter Zuhilfenahme eines Smartphones bestimmt. Dazu wurden im Versuchsaufbau die Naheinstellgrenze empirisch evaluiert und die resultierenden Fingerprintaufnahmen näher untersucht. Während die Erkenntnisse natürlich ein Smartphone-/Kameraspezifisches Ergebnis darstellen, waren vor allem der generelle Umgang und die Machbarkeit einer derartigen Aufnahmetechnik von Interesse. Bei den Bildern stellten sich folgende Betrachtungen (unter Bezugnahme auf das getestete Phone Samsung Galaxy Note 4):

- Fingeraufnahmen lassen sich mit ausreichender optischer Qualität nah ab ca. 8,5 cm bis ca. fern: 16,5 cm erstellen, wobei bei Nahaufnahmen die Naheinstellgrenze und bei Fernaufnahmen die ausreichende Beleuchtung sowie Auflösung eine natürliche Machbarkeitsbarriere darstellen.
- Autofokussierung speziell bei Naheinstellungen erwies sich in der Praxis als fehleranfällig mit Fehlfokussierungen als Folge (weshalb in weiterer Folge als Aufnahmeverfahren auch ein fixer Fokus mit Aufnahme mehrerer Bilder mit variierender Distanz zum Sensor in Betracht gezogen wurde). Derartige Fehlfokussierungen können vermieden werden, indem eine Programmierschnittstelle verwendet wird, die weitere Parameter zur Fokussierung (z.B. Fokussierungsbereich etc.) zulässt.
- Ideale Aufnahmedistanz: ca. 10 cm.
- Die Parameter, welche signifikante Auswirkung auf die erhaltene Bildqualität haben, sind: Fokus vs. Ausleuchtung vs. Auflösung.

Beim Vergleich zweier verschiedener Smartphones ergaben sich folgende Analysen:

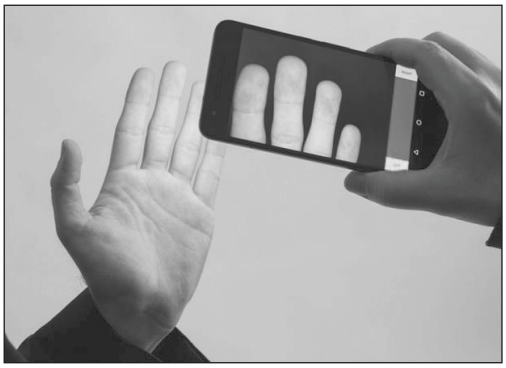
Note 4:

- bessere Auflösung (16 MP),
- akkurate automatische Fokussierung,
- integrierter Blitz liefert keine so gute Ausleuchtung.

Nexus 6:

- gute Auflösung (13 MP),
- nicht so leichtgängiger automatischer Fokus,
- Ringbeleuchtung liefert sehr gute Bildqualität.

Quelle: Modentity Konsortium



Aufnahme von vier Fingerabdrücken gleichzeitig durch Abfilmen mittels Smartphonekamera

Quelle: Modentity Konsortium

Anzeige der Qualität der erfassten Fingerabdrücke

4.3 Segmentierung

Um eine schnelle Fingerabdruckverarbeitung vornehmen zu können, müssen Finger schnell von Hintergrundinformation separiert und deren Position und Lage bestimmt („segmentiert") werden. Je nach Komplexität des Hintergrunds gestaltet sich diese Aufgabe als herausfordernd. Bei einheitlichem dunklen Hintergrund können Thresholding-Verfahren verwendet werden, dies ist jedoch im geplanten Einsatzgebiet nicht ausreichend (z.B. Boden als Hintergrund, Büromöbel etc.) welche stärkere Kanteninformation im Hintergrund aufweisen). Die Implementierung eines Algorithmus erfolgte basierend auf Hautfarbe, jedoch wurden speziell einfache und schnell berechnete Masken zu diesem Zweck entwickelt sowie ein iterativer Ansatz gewählt, um den Einfluss der Kamera/des Smartphones auf die Segmentierungsleistung möglichst zu kontrollieren.

Verschiedene Masken werden dazu in einem Fusionsprozess kombiniert und eine Segmentierung des Bildes in Fingerabdruck und Hintergrund vorgenommen. Einzelne Finger werden mittels Konturen erkannt und ein rechteckiges orientiertes Fenster („bounding box") um den Finger definiert die zu extrahierenden Regionen, welche vom Algorithmus erkannt und als individuelle Fingerbilder aus der Einzelaufnahme herausgerechnet werden. Insbesondere wurden Masken entwickelt, welche auch die Trennung von Fingern ermöglichen, die einander während der Aufnahme berühren – eine Spreizung der Finger oder Einzelfingeraufnahme ist somit im Gegensatz zu aktuellen Verfahren nicht erforderlich. Als wesentlichen Schritt vor der weiteren Verarbeitung wird die Auflösung mittels Ridge Frequency geschätzt.

4.4 Bildverbesserungsverfahren

Nach erfolgreicher Identifizierung und geeigneter Rotation der Bilder einzelner Fingerabdrücke müssen diese geeignet aufbereitet werden, um eine weitere Verarbeitung durch einen automationsgestützten Algorithmus zu ermöglichen. Dazu ist es notwendig, dass die Darstellung der Fingerabdrücke möglichst jenen von optischen FTIR (frustrated total internal reflection) bzw. kapazitativen Fingerprint Sensoren entspricht, welche Fingerabdrücke aufnehmen, die eine Oberfläche berühren. Bei derartigen Verfahren ist der Kontrast zwischen „Ridges" und „Valleys"

typischerweise stark ausgeprägt. Ziel des Bildverbesserungsverfahrens ist die Erreichung der Charakteristika derartiger Touch-Sensoren.

Das Verfahren verbessert den Kontrast der „Ridges" mittels Mean/Variance Normalisierung, Normalized Box Filtern sowie morphologischen Operationen und identifiziert Regionen mit schwachem Kontrast.

4.5 Merkmalsextraktion und Vergleich

Während für die Basisfunktionalität der Fingerabdruckaufnahme ein geeignetes Bild des Fingerabdrucks gewonnen werden muss und keine Einflussmöglichkeit auf weitere Verarbeitungsschritte besteht (z.B. für Abgleich mit externen Systemen, wie VISA-Informationssystem oder EURODAC[3]), so ist dennoch die Implementierung und Anbindung von Merkmalsextraktions- bzw. Vergleichsalgorithmen sehr sinnvoll. Einerseits ergibt sich erst dadurch die Möglichkeit, die Eignung der Bilder für den biometrischen Vergleich festzustellen, andererseits würde dadurch im hypothetischen Fall, dass mittels eines verfügbaren Zertifikats ein auf einem Dokument hinterlegter Fingerabdruck ausgelesen werden könnte, ein Merkmalsvergleich gleich direkt am Gerät stattfinden.

Um eine kostengünstige und praktische Auswertung von Fingerprints zu ermöglichen, wurde die Anbindung der Open Source Fingerabdruckssoftware NBIS (NIST Biometric Imaging Software) vorgenommen, speziell wurde eine Einbettung der Algorithmen „mindtct" für den Merkmalsextraktionsprozess sowie „bozorth" für den Vergleichsprozess implementiert. Dazu wurden eigene Container zur effizienten Speicherung und Ablage geschaffen, welche x y t q (Position, Orientierung, Qualität) von charakterisierenden Minutien speichern.

4.6 Zusammenfassung und Ausblick der Fingerprintaufnahme

In diesem Arbeitspaket gelang es ein voll funktionsfähiges Verarbeitungssystem für Fingerprintabdrücke aus der Distanz mittels Smartphones zu verwirklichen. Die Skalierung der Fingerabdrücke auf eine Zielauflösung von 500 dpi funktionierte nur annäherungsweise (siehe Studie im Paper Wild et al. 2016), eine tolerantere Skalierungsinvarianz sollte vom Vergleichsalgorithmus bereitgestellt werden. Grund für die ungenaue Schätzung ist die (relative) Streuung der Frequenz der Papillarleisten zwischen verschiedenen Individuen (so ist z.B. auch eine Abweichung zwischen männlichen und weiblichen Fingern in der Literatur evident). Immerhin könnte die Skalierung deutlich besser geschätzt werden, wenn ein Originalfingerabdruck oder weitere Information zum betreffenden Finger zur Verfügung steht. Insgesamt erzielte die implementierte Verarbeitungskette mit Post-feature Extraction Scaling invariance unter 1 % EER für den Cross-Phone-Vergleich und für Verifikationsanwendungen ausreichend hohe GAR (> 97% GAR bei 0,1% FAR für Flex 2).

5. GSK-ASPEKTE[4]

5.1 Einsatzkontext

Der anvisierte Einsatzkontext der Modentity-Geräte liegt im Rahmen von Personen- und Dokumentenkontrollen, speziell als unterstützendes Werkzeug innerhalb der so genannten Ausgleichsmaßnahmen (AGM[5]). Die Desk Research hat eine Reihe von Kritikpunkten an den AGM aufgezeigt: Sie seien Teil des Überwachungsstaats, es gäbe uneinheitliche Regelungen in der EU bzw. in den Schengen-Staaten dazu, sie seien unverhältnismäßig, und durch Einführung der AGM habe es letztendlich keinen tatsächlichen Wegfall von Grenzkontrollen gegeben. Zudem lautet ein häufiger Vor-

wurf an AGM-Beamte auf Grund äußerer Merkmale von zu kontrollierenden Personen aktiv zu werden (racial/ethnic bzw. social profiling). Ein wichtiger Vorschlag, um einen Teil dieser Vorwürfe zu adressieren, ist Transparenz bei der Einführung neuer Sicherheitstechnologien oder Überwachungspraktiken herzustellen und klare und verständliche Regelungen zu deren Zweck, Art und Häufigkeit aufzustellen.

Die quantitative Befragung hat gezeigt, dass die Akzeptanz gegenüber der Modentity-Technologie danach variiert, je nachdem, wie wichtig die Polizei, Kontrollen und eine entsprechende Ausrüstung für die Aufrechterhaltung der Sicherheit in Österreich betrachtet werden. Beim überwiegenden Teil der Bevölkerung werden diese Aspekte für sehr wichtig eingeschätzt. Quantitativ betrachtet tendiert die österreichische Bevölkerung aber gemessen an unseren Befragungsergebnissen dazu, die Modentity-Technologie eher zu akzeptieren.

Während laut Desk Research eine Gesellschaft mit eher hohem subjektiven Sicherheitsgefühl geringere Akzeptanz gegenüber neuen Überwachungs- und Kontrolltechnologien aufweist und in Österreich das subjektive Sicherheitsgefühl im Schnitt immer noch eher hoch ist, so zeigt das Sicherheitsmonitoring, dass es hier seit Jahren einen negativen Trend gibt und Unsicherheiten in der Bevölkerung in Bezug auf Flüchtlinge, Grenzsicherung und irreguläre Migration bestehen. Laut Desk Research wirkt sich auch ein hohes Maß an (wahrgenommener) Einwanderung eher positiv auf die Akzeptanz aus.

Die quantitative Befragung hat zudem gezeigt, dass der österreichische Staat und seine Behörden beim Großteil der Bevölkerung in Bezug auf staatlichen Datenschutz und staatliche Integrität in der Datenverarbeitung großes Vertrauen genießen. Dies wirkt sich positiv auf die Akzeptanz gegenüber der Technologie aus.

Weitere soziale Einflussfaktoren, die mit der zu erwarteten Akzeptanz gegenüber Sicherheitstechnologien zusammenhängen, umfassen laut Desk Research die allgemeine Aufgeschlossenheit gegenüber neuen Technologien im Allgemeinen sowie das Image der neuen Sicherheitstechnologie, wobei sowohl Österreich bezüglich der Technologisierung (festgemacht am Grad der Verbreitung des Internets) im EU-Schnitt liegt und Smartphones bereits etablierter Bestandteil des Alltags für viele Menschen sind.

Die Fokusgruppe mit den Polizeibeamtinnen und -beamten hat darauf verwiesen, dass die aktuelle Ausstattung der im AGM-Bereich tätigen Polizistinnen und Polizisten als mangelhaft wahrgenommen wird und die generelle Einstellung gegenüber der Modentity-Technologie sehr positiv ist. Es besteht die Hoffnung, dass Modentity-Devices gegenüber den bestehenden Einsatzlaptops bzw. der Praxis, mit stationären Beamtinnen und Beamten Kontakt zwecks Auskünfte aufzunehmen den Vorteil haben, rascheren und stabileren Zugriff auf Datenbanken zu erlauben und weitere Sicherheitsmerkmale von Dokumenten zu erfassen, um mit den immer ausgefeilteren Methoden der Dokumentenfälscherinnen und -fälscher Schritt zu halten. Besonders nach Schulungen, die erste Kontaktängste mit der neuen Technologie nehmen und nach ersten Erfolgserlebnissen dürfte die Akzeptanz seitens der Anwenderinnen und Anwender eher hoch sein.

5.2 Einsatzsituation

Die Modentity bezogene Einsatzsituation als soziale Mikrosituation beginnt dann, wenn Beamtinnen und Beamte mit zu kontrollierenden Personen in Interaktion treten und Modentity-Geräte als unterstützendes Werkzeug einsetzen, um diese Personen oder ihre Dokumente zu überprüfen. Die

Fokusgruppen und die Expertengespräche haben die Bedeutung und Fragilität dieser Situation hervorgehoben, und dass die Akzeptanz der Bevölkerung maßgeblich von der Ausgestaltung dieser Situation abhängt.

Aus Sicht der befragten Expertinnen und Experten wurde die Gefahr einer neuen sozialen Situation durch Einbezug der Geräte stark gemacht (etwa weil diese beim Fotografieren der Person als symbolische und physische Barriere zwischen Kontrollorgan und kontrollierter Person stehen), die von zahlreichen Unklarheiten für die von der Kontrolle Betroffenen geprägt ist (Was passiert mit den Daten? Warum werde ich dergestalt kontrolliert?). Verstärkt werden diese Unklarheiten im Falle von AGM noch, dass hier die Chance größer ist, dass Personen kontrolliert werden, die entweder schlecht oder gar nicht Deutsch können und womöglich (auch in ihrer Muttersprache) nicht alphabetisiert sind. Der Vorschlag von Expertinnen- und Expertenseite, die Displays der Modentity-Geräte vorzeigbar zu gestalten, damit Beamtinnen und Beamte die Betroffenen durch den Prüfprozess führen können, ist zwar ein wichtiger Schritt, stößt aber im Falle von nicht-alphabetisierten Personen, sofern schriftliche Elemente einbezogen werden, an ihre Grenzen.

Zweitens wurde darauf hingewiesen, dass es eine Reihe von besonders vulnerablen Personen mit erhöhtem objektiven und/oder subjektiven Datenschutzbedürfnis gibt, die von den Möglichkeiten einer biometrieunterstützten Kontrolle besonders betroffen sein können. Beispielsweise sind das Personen, die generell polizeikritisch sind (etwa weil sie öfters auf Demonstrationen waren und dort einschlägig schlechte Erfahrungen gemacht haben), die Migrationshintergrund aufweisen und durch Racial-Profiling-geprägte Praktiken öfters Kontrollen unterworfen sind, datenschutzsensible Personen oder auch traumatisierte Personen mit Fluchterfahrung, die einen eigenen sozialen Umgang erfordern. Politisch verfolgte Personen, die in Österreich Asyl suchen oder aus anderen berechtigten Gründen nicht gefunden werden möchten, können sich durch den Einbezug biometrischer Merkmale besonders leicht identifizierbar fühlen, speziell wenn sie im Unklaren über die genaue Datenverwendung sind und darüber, ob verschiedene Datenbanken gebündelt werden (und damit z.B. auch Geschlechtsumwandlungen anhand des Fingerabdrucks nachvollziehbar machen, was für Betroffene besonders unangenehm sein kann).

Mehrmals hervorgehoben wurde von den Expertinnen und Experten daher die Notwendigkeit, dass spezielle Schulungen die Beamtinnen und Beamte auf den Einsatz der Geräte vorbereiten, und zwar nicht nur bezüglich der technischen Anwendung, sondern ebenso hinsichtlich eines sensiblen, kommunikativ-sozialen Einsatzes dieser Geräte. Es geht darum, die Beamtinnen und Beamten auf zahlreiche neue Effekte und Fallstricke hinzuweisen, die in der Kontrollsituation für sie selbst und für die Bevölkerung eintreten können. Gerade wenn man eine eher rigide Befehlsstruktur gewohnt ist, besteht womöglich die Gefahr, neue Technologien schematisch anzuwenden und interaktive Aspekte zu vernachlässigen. Hier entsteht freilich ein Zielkonflikt zwischen ausreichend Aufklärung in der Kontrollsituation über das Prozedere und einem ausreichend effizienten Vorgehen, besonders nach einem bereits langen Arbeitstag in einem immer potentiell gefährlichen Arbeitsumfeld.

Auch die Bevölkerungsfokusgruppen und die quantitative Befragung unterstreichen die Notwendigkeit eines höflichen, geduldigen Umgangs der Beamtinnen und Beamten mit den Betroffenen, mit ausreichend begleitenden Erklärungen oder

wie ein Diskussionsteilnehmer es auf den Punkt brachte: „Der Ton macht die Musik". Zunächst fehlende Akzeptanz gegenüber einer neuen Kontrolltechnologie kann und muss daher immer zu einem gewissen Teil durch die kommunikative Kompetenz der Anwenderinnen und Anwender ausgeglichen werden.

6. ZUSAMMENFASSUNG DER PROJEKTERGEBNISSE

Im Projekt Modentity wurde gemeinsam mit der Polizei ein fortschrittliches System entwickelt, das es erlaubt, Personenkontrollen mittels Smartphones durchzuführen. Hierbei wird auf COTS (commercial of the shelf) Komponenten zurückgegriffen. Die Softwareentwicklung nahm den Großteil der Arbeiten ein. Es entstand ein Modulsystem auf Androidbasis um:

- die MRZ in eMRTD's (electronic Machine Readable Travel Document, z.B. Pass) zu lesen,
- den Chip des eMRTD auszulesen und auf Gültigkeit zu prüfen,
- das Gesicht des Reisenden mit dem im eMRTD gespeicherten zu vergleichen,
- Fingerprints von Reisenden mit guter Qualität kontaktlos aufzunehmen,
- Speicherung der nicht abgeschlossenen Verifikationsvorgänge, um bei Verbindungsabriss unmittelbar fortsetzen zu können.

Je nach verfügbarer Funktionalitätsdichte kann die in Modentity entwickelte Lösung auch von unterschiedlichen Benutzergruppen, wie Grenzkontrollbeamten, Polizei oder Armee und Blaulichtorganisationen, im Krisenfall für ihre spezifischen Aufgaben eingesetzt werden.

Bezüglich GSK- und Datenschutzanforderungen gibt es hinsichtlich des Einsatzes von Modentity sehr positive Signale. Die erarbeiteten Ergebnisse stellen Schulung der Anwender, Information der Bevölkerung und gute Kommunikation als wichtigste Eckpfeiler für die Zukunft dar. Das parallel zu Modentity in Auftrag gegebene Rechtsgutachten findet keine Hindernisse zur Anwendung bei Einhaltung der gesetzlichen Bedingungen, state-of-the-art Datenschutz vorausgesetzt.

[1] *ICAO (International Civil Aviation Organization).*

[2] *RFID (radio-frequency identification): Identifizierung mit Hilfe elektromagnetischer Wellen) bezeichnet eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.*

[3] *EURODAC (European Dactyloscopy): ist ein Fingerabdruck-Identifizierungssystem für den Abgleich der Fingerabdruckdaten aller Asylwerberinnen und Asylbewerber sowie von bestimmten Drittstaatsangehörigen und Staatenlosen, wenn die betreffenden Personen älter als 14 Jahre sind.*

[4] *Geistes-, sozial- und kulturwissenschaftliche Aspekte.*

[5] *AGM (Ausgleichmaßnahmen): Ausgleichsmaßnahmen sind Maßnahmen im Binnenland zur Verhinderung und Bekämpfung spezifischer kriminal-, fremden- und verwaltungspolizeilicher Delikte nach dem Wegfall der Grenzkontrollen.*

Quellenangaben

Wild, Peter et al. (2016, im Erscheinen). Comparative Test of Smartphone Fingerphoto vs. Touch-based Cross-sensor Fingerprint Recognition, Journal IET Biometrics o.V.

Weiterführende Literatur und Links

AIT [Austrian Institute of Technology] et al. (2013). Future Border Control, Bericht AP 2 – Usability, Legal and Social Aspects, KIRAS Sicherheitsforschung, Wien.

Baier, Harald/Straub, Tobias (2008). Vom elektronischen Reisepass zum Personalausweis: RFID und personenbezogene Daten – Lessons Learned!?, in: Fischer, Stefan et al. (Hg.) Informatik 2009 – Im Focus des Lebens, Bonn, Online: http://subs.emis.de/LNI/Proceedings/

Proceedings154/gi-proc-154-135.pdf (04.02.2012).

Beuth, Patrick (2014). Hacker kopieren 270.000 Datensätze der deutschen Polizei, Die Zeit, 17.01.2014, Online: http://www.zeit.de/digital/datenschutz/2014-01/hacker-kopieren-daten-schengener-informationssystem (18.02.2015).

Bezirksblatt (2011). Schlangen in PKW entdeckt, 14.03.2011, Online: http://www.meinbezirk.at/berwang/chronik/schlangen-in-pkw-entdeckt-d56145.html (15.02.2015).

Bezirksblatt (2013). Polizeiinspektion Nickelsdorf AGM – erfolgreiche Arbeit im Kampf gegen die Kriminalität, 14.02.2013, Online: http://www.meinbezirk.at/apetlon/chronik/polizeiinspektion-nickelsdorf-agm-erfolgreiche-arbeit-im-kampf-gegen-die-kriminalitaet-d507294.html (15.02.2015).

Bezirksblatt (2014). Zwölf Flüchtlinge in Bruck an der Leitha aufgegriffen, 17.07.2014, Online: http://www.meinbezirk.at/bruck-an-der-leitha/chronik/zwoelf-fluechtlinge-in-bruck-an-der-leitha-aufgegriffen-d1022504.html (15.02.2015).

Biermann, Kai (2013). Polizei in San Diego testet Gesichtserkennung, Die Zeit, 08.11.2013, Online: http://www.zeit.de/digital/datenschutz/2013-11/usa-polizei-gesichtserkennung (19.02.2015).

Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung [BAK] (2013). Polizeiinspektion und AGM-Dienststelle am Wiener Hauptbahnhof eröffnet, Online: http://www.bak.gv.at/cms/BAK_en/_news/BMI.aspx?id=4A5266654C4B6A7232356B3D&page=1&view=1 (16.02.2015).

C-188/10 und C-189/10 Aziz Melki und Selim Abdeli, Urteil vom 22. Juni 2010: http://ec.europa.eu/dgs/legal_service/arrets/10c188_de.pdf (25.02.2015).

CP WISSEN (2014). Bitkom: Hohe Akzeptanz für biometrische Daten, 17.08.2014, Online: http://www.cpwissen.de/Online/items/bitkom-hohe-akzeptanz-fuer-biometrische-daten.html (02.03.2015).

Cremer, Hendrik (2013). Racial Profiling. Menschenrechtswidrige Personenkontrollen nach § 22 Abs. 1a Bundespolizeigesetz. Empfehlungen an den Gesetzgeber, Gerichte und Polizei, Berlin.

Datenschutz Forum (2009). Beitrag Peter Schaar, 13.07.2009, Online: https://www.bfdi.bund.de/bfdi_forum/showthread.php?t=4112 (18.02.2015).

Dernbach, Andrea (2014). Gericht hält Zug-Kontrollen ohne Anlass für rechtswidrig, Der Tagesspiegel, 10.11.2014, Online: http://www.tagesspiegel.de/politik/racial-profiling-gericht.

FastPass, Projekt & Konsortium, 2013–2017, Harmonisierung in der automatisierten Grenzkontrolle, Online: www.FastPass-project.eu.

MobilePass, Projekt & Konsortium, 2014–2016, Dedizierte Geräteentwicklung für mobile Grenzkontrolle, Online: www.MobilePass-project.eu.

Orczyk, Tomasz/Wieclaw, Lukasz (2011). Fingerprint ridges frequency, Third World Congress on Nature and Biologically Inspired Computing, Salamanca, 558–561.

Sankaran, Anush et al. (2015). On smartphone camera based fingerphoto authentication, Proc. Int'l. Conf. Biometrics Theory, Appl. and Systems (BTAS), Delih, 1–7.

Stein, Chris (2012). Fingerphoto recognition with smartphone cameras, Proc. Conf. Biometrics Special Interest Group (BIOSIG), Darmstadt, 1–12 .

Yulong, Zhan et al. (2015). Fingerprints On Mobile Devices: Abusing and Leaking, Black Hat Conference 2015.