Protect-It_Nr_15_Layout 1 12.04.10 13:30 Seite 35

BIOMETRISCHE PÄSSE

Kantonspolizei Zürich
Urkundenlabor

▲ *ICAO-Symbol für elektronische maschinenlesbare Identitätsdokumente.*

▲ *rot = kein Zugriff auf Daten*

▲ *grün = «echt»*

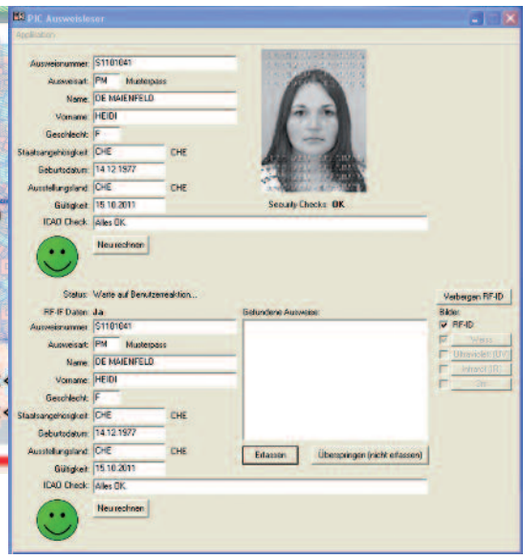
Sind sie fälschungssicher?
Ende 2009 stellten weltweit über 80 Staaten biometrische Pässe her. In diesen Dokumenten werden biometrische Merkmale (zum Beispiel Fotografie, Fingerabdrücke, Iris) sowie einige Passdaten des Ausweisinhabers auf einem Mikroprozessor (Chip) gespeichert. Dieser Chip befindet sich in der Regel im Einband oder in der Personalienseite. Biometrische Pässe sind mit einem international verwendeten Symbol auf der Vorderseite gekennzeichnet.

Als assoziierter Schengen-Staat ist die Schweiz verpflichtet, spätestens ab dem 1. März 2010 nur noch Pässe mit elektronisch gespeichertem Gesichtsbild und zwei Fingerabdrücken auszustellen. Die im Pass 10 gespeicherten Daten sind durch ein mehrstufiges gesichertes Zugriffsverfahren und elektronische «Schlüssel» geschützt. Damit ein anderes Land spezielle Files (zum Beispiel Fingerabdrücke) überhaupt lesen kann, muss es über die Berechtigung der Schweiz verfügen.

Wie erfolgt die Kontrolle?
Der zu überprüfende Reisepass wird auf ein Pass-Lesegerät gelegt. Damit der Zugriff auf die biometrischen Daten des Chips freigegeben werden kann, liest das Gerät zuerst die maschinenlesbare Zone MRZ (zwei Zeilen im unteren Bereich der Personalienseite) und überprüft die innerhalb dieser Zeilen enthaltenen Kontrollziffern auf Plausibilität. Stellt das Gerät in der MRZ Fehler fest oder kann es diese Zeilen aus einem anderen Grund (zum Beispiel Verschmutzung) nicht lesen, wird der Zugang zu den Daten im Chip nicht freigegeben (rotes Emblem). Falls das Gerät keine Daten überträgt, könnte dies darauf hinweisen, dass der Chip beschädigt ist bzw. dass am Chip Manipulationen vorgenommen worden sind oder eine Fälschung vorliegt.

Ist die MRZ korrekt und stimmen die Plausibilitätsziffern, kann das Pass-Lesegerät das File auf dem Chip öffnen und die für den jeweiligen Anwender zugänglichen biometrischen Daten auf einen Bildschirm übertragen (grünes Emblem zeigt O.K.).

▲ *Biometrischer Reisepass.*



▲ *Unten Daten der MRZ-Zeile; oben Chip-Daten Lesegerät zeigt O.K. (grüne Embleme).*

Protect-It_Nr_15_Layout 1 12.04.10 13:30 Seite 36

Ist der Pass nun auch O.K.?
Die Praxis zeigt, dass auch biometrische Pässe von Fälschungen nicht ausgenommen sind. Dabei wird nicht der Chip bzw. die im Chip eingelesenen Files manipuliert, sondern beispielsweise das im Pass befindliche Bild bzw. die Personalienseite gefälscht. Bei der Prüfung muss deshalb das auf dem Chip gespeicherte Bild mit dem Passbild auf der Personalienseite verglichen werden. Weiter müssen bei Dokumenten mit biometrischen Daten nebst dem Bild auch die übrigen Passdaten auf Fälschungsmerkmale überprüft werden (zum Beispiel Geburtsdatum, Gültigkeitsdauer, Visa etc.).

Die Einführung der biometrischen Daten und die Speicherung auf einem Chip sind ein weiteres Glied in der ganzen Sicherheitskette eines Dokumentes der neueren Generation. Das Entschlüsselungsgerät kann Daten auf einem Chip einsehen und zum Teil mit den Einträgen in der MRZ vergleichen. Trotz dieser Möglichkeit ist es jedoch unerlässlich – wenn das Gerät «echt» anzeigt (zwei Mal grün) –, einen biometrischen Ausweis wie bis anhin auf Fälschungsmerkmale zu prüfen.

▼ *Übersicht einer verfälschten Personalienseite.*

▲ *Dieses Beispiel einer Bildmanipulation zeigt, dass es unerlässlich ist, bei der Prüfung eines biometrischen Reisepasses mittels des Pass-Lesegerätes, das auf dem Chip gespeicherte Bild mit dem Passbild auf der Personalienseite zu vergleichen.*

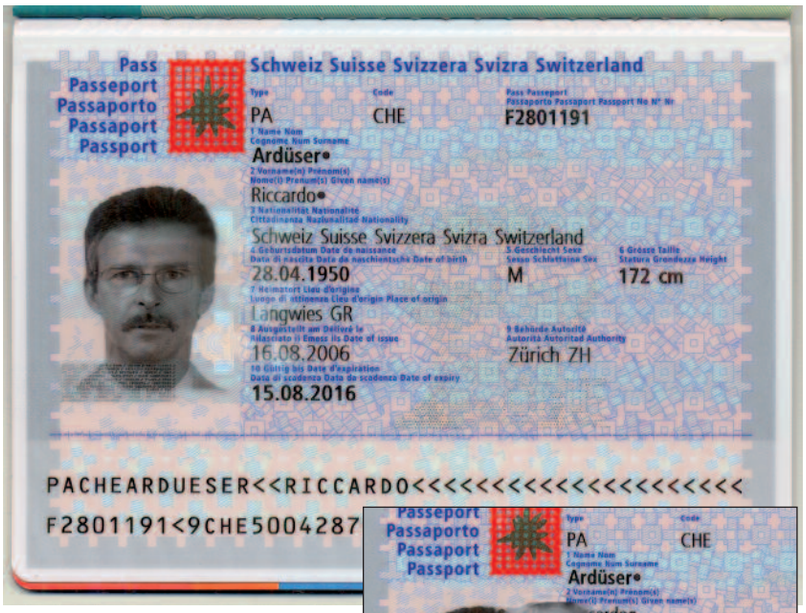
▲ *Die Prüfung auf dem Passlesegerät zeigt: MRZ und Chip sind O.K. (grüne Embleme).*

▲ *Bild auf Chip.*

▲ *Zusätzlich zur Bildmanipulation wurde auch die Grössenangabe verändert.*

Protect-It_Nr_15_Layout 1 12.04.10 13:30 Seite 37

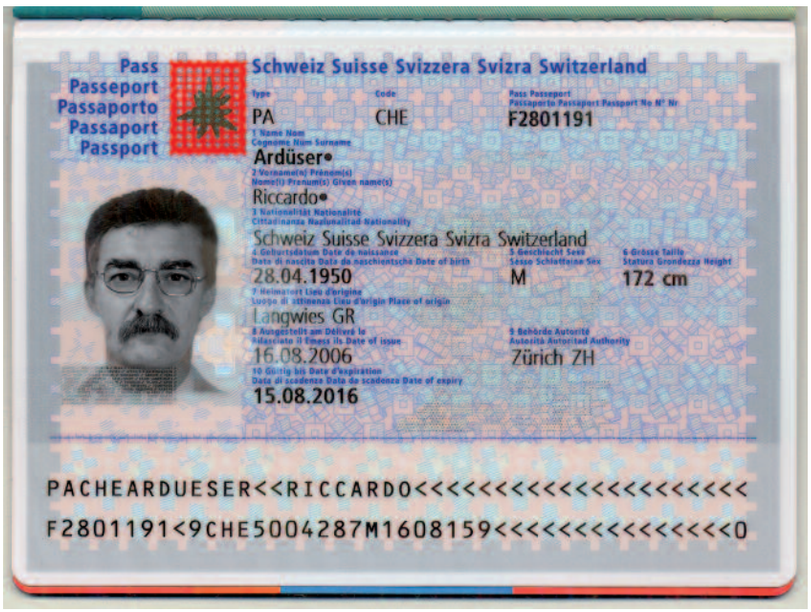
Beispiel über das Vorgehen einer neuartigen Passfälschung



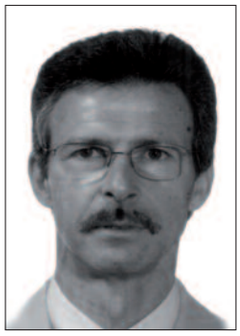
▲ *Unverfälschte Personalienseite.*

▲ *Austausch des Gesichtsfeldes.*

▲ *Fälscherbild.*



▲ *Verfälschte Personalienseite.*



▲ *Ursprünglicher Ausweisinhaber; Bild auf Chip.*

Dieses Beispiel einer Bildmanipulation zeigt, dass es unerlässlich ist, bei der Prüfung eines biometrischen Reisepasses mittels des Pass-Lesegerätes, das auf dem Chip gespeicherte Bild mit dem Passbild auf der Personalienseite zu vergleichen.