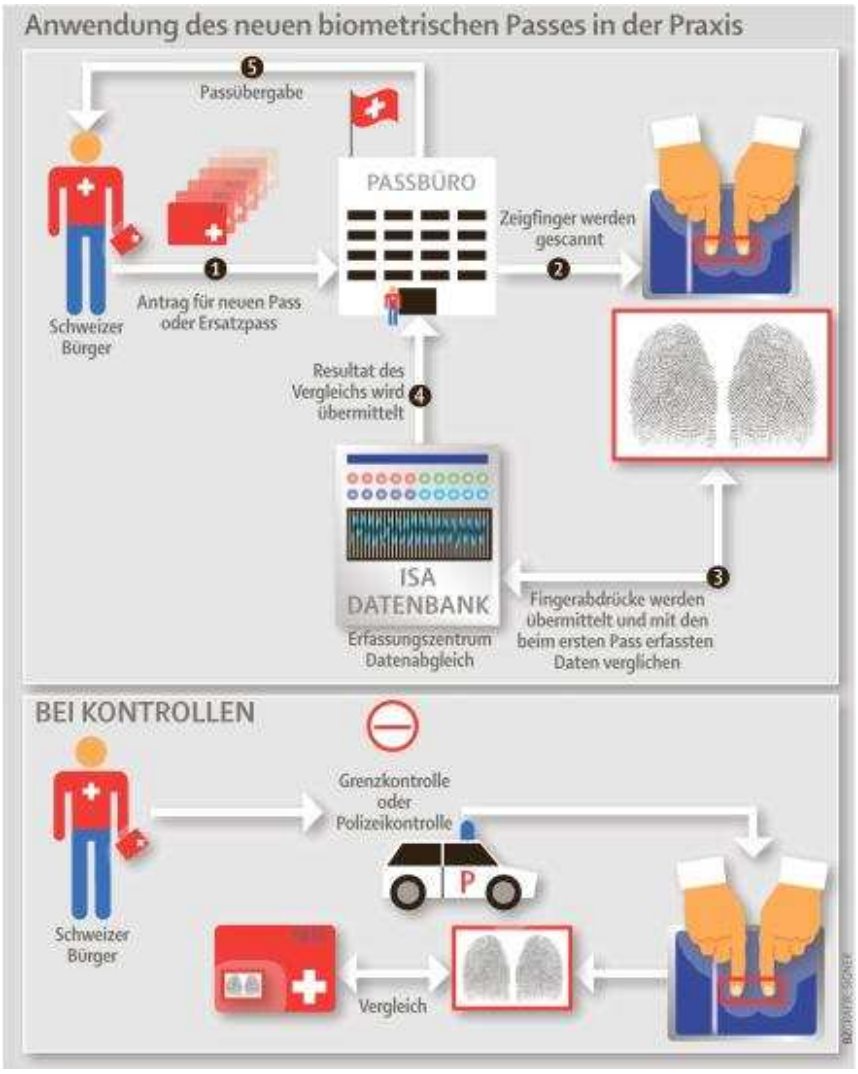
Tages-Anzeiger SCHWEIZ

Darum gehts beim umstrittenen Pass wirklich

Aktualisiert am 18.04.2009 **80 Kommentare**

Kriminelle könnten die biometrischen Daten des neuen Passes unbemerkt lesen und die Reisen des Passinhabers verfolgen, wird behauptet. Doch tatsächlich lassen die technischen Möglichkeiten des Passes dies nicht zu.



Artikel zum Thema

Biometrischer Pass: «Strassburg» als Joker

Im neuen biometrischen Pass (Pass 10), über den das Voll am 17.Mai abstimmt, löst vor allem der mit Sender und Antenne ausgestattete RFID-Chip Ängste aus. Im Abstimmungskampf kursieren diffuse Befürchtungen übe die technischen Möglichkeiten, die bis hin zur totalen Überwachung des Passinhabers gehen. Der schon erhältliche Pass 06 ist auch mit einem solchen

Chip ausgerüstet – hier gab es diese Befürchtungen nicht. Der Chip im neuen Pass enthält allerdings zusätzlich Fingerabdrücke und ist besser geschützt, ansonsten gibt es kaum Unterschiede. Auch äusserlich sehen die beiden Pässe gleich aus.

RFID ist die Abkürzung für «Radio Frequency Identification», auf Deutsch heisst das: Identifikation mittels elektromagnetischen Wellen. Im biometrischen Pass wird ein passiver RFID-Chip zwischen zusammengeklebten Kunststoffseiten im Deckel eingebaut. Passiv bedeutet, dass der Chip nicht durch eine eigene Batterie betrieben wird. Aktivieren lässt er sich mit einem Lesegerät, das über ein externes Magnetfeld verfügt. Dies ist auch bei geschlossenem Pass möglich. Doch der etwa fingernagelgrosse Chip, der von einer rechteckigen, deutlich grösseren Funkantenne umgeben wird, kann nur aus einer geringen Distanz von maximal 20 Zentimetern aktiviert und gelesen werden. «In der Praxis beträgt die Distanz eher 10 Zentimeter», sagt Markus Waldner, Projektleiter Biometrie, beim Bundesamt für Polizei (fedpol). Es ist also nicht möglich, die persönlichen Daten aus grosser Distanz unbemerkt abzurufen.

Wenn der RFID-Chip über einen Magnetfeldleser zum Leben erweckt wird, sendet er zur Begrüssung von Mal zu Mal eine neue Nummer aus. Dann wartet er jeweils auf eine Antwort. Erst wenn er den passenden Schlüssel erhält, beginnt der Chip im sogenannten Basic-Access-Control-Verfahren (BAC) zu kommunizieren. Nach dem Überwinden dieser Hürde gibt der Chip nur jene Daten frei, die ohnehin im Pass lesbar sind.

Komplexer Schlüssel

Der BAC-Schlüssel lässt sich allerdings nicht einfach überwinden. Er setzt sich zusammen aus einer siebenstelligen Passnummer, dem Geburtsdatum und dem Ablaufdatum des Passes. Selbst bei einer einigermassen genauen Schätzung von Alter des Inhabers und Ablaufdatum kann dieser Code laut Waldner erst nach etlichen Jahren ununterbrochener Versuche geknackt werden, und der Angreifer erhielte dann lediglich die erwähnten Daten, die ohnehin auf der Personalienseite des Passes stehen. Das lässt die Befürchtungen eines solchen Datenklaus realitätsfern erscheinen. Denn wer auf wenige Zentimeter an den Pass herankommt, wird die Angaben eher kopieren oder mit dem Handy eine Foto machen, als versuchen, den Code zu knacken.

Drei Datengruppen

Die Daten sind im neuen biometrischen Pass in drei verschiedenen Gruppen abgelegt. Die erste Gruppe enthält alle Angaben, die im Pass lesbar sind – mit Ausnahme der Foto und der Fingerabdrücke. In der zweiten Gruppe wird die Foto in der gleichen Grösse wie die Originalfoto gespeichert. Die dritte Gruppe enthält zwei Fingerabdrücke. In der Regel sind dies die Abdrücke der beiden Zeigefinger. Stets sind flache Abdrücke gespeichert. Die Polizei verwendet hingegen gerollte Fingerabdrücke von allen zehn Fingern, um eine zuverlässigere Identifikation zu ermöglichen. Für Fahndungszwecke wären diese Daten deshalb nur bedingt tauglich. Weitere Angaben wie beispielsweise zum Reiseverhalten des Passinhabers werden im Chip des neuen biometrischen

Passes nicht gespeichert.

Schwieriger ist der Zugriff auf die gespeicherten Fingerabdrücke. Im neuen Pass kommt hier das Extended-Access-Control-Verfahren (EAC) zur Anwendung. Damit der RFID-Chip diese Daten frei gibt, muss das Lesegerät einen weiteren Code senden. Dabei handelt es sich um ein Zertifikat, das ar ausgewählte Länder vergeben und in Abständen von zwei Wochen bis maximal drei Monaten erneuert wird. Die Schweiz kann also den Zugriff auf die Fingerabdrücke stoppen, indem sie Zertifikate für bestimmte Länder nicht mehr erneuert.

Klonen nicht möglich

Lesbare Daten können auch kopiert werden. Diese Regel ist im Bereich der Ausweisfälschung von Bedeutung: Mit einmal gelesenen Daten lassen sich demnach neue Pässe mit anderen Fotos herstellen. Der neue biometrische Pass verhindere einen solchen Missbrauch, versichert Waldner. Der Grund: «Der Chip enthält einen weiteren geheimen Schlüssel, der nicht kopierbar ist.» Ohne diesen Code wird bei einer Kontrolle festgestellt, dass mit dem Ausweis etwas nicht in Ordnung ist.

Zusätzlich sind die Daten im Chip elektronisch signiert, sodass auch eine Veränderung bemerkt würde. Hinzu kommt schliesslich, dass für einen Missbrauch auch das Passbüchlein, in welches der Chip eingebaut werden soll, gefälscht werden müsste. (Bernhard Kislig/bz)

Erstellt: 18.04.2009, 10:07 Uhr