Innenausschuss
A-Drs. 16(4)192 B

Stellungnahme der DN Systems Enterprise Internet Solutions GmbH, Hildesheim

Anmerkungen zum Passgesetz und zur Realisierung der MTRD (Machine Readable Travel Document) nach ICAO Standard

Die im Entwurf zur Änderung des Passgesetzes aufgestellten Anforderungen in §4 Absatz 3

„Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern“

sind nach der Spezifikation der ICAO, weder mit Basic Access Control (BAC) noch mit Extended Access Control (EAC), nicht zu erfüllen.

Die ICAO Spezifikation steht konträr zu den „Best Practices“ für die Absicherung von Informationssystemen und beinhaltet drei Risiken:

1. Es besteht das Risiko, dass in das geschlossene Inspektions-System, das heute auf dem rein optischen Auslesen der maschinenlesbaren Zone (MRZ) basiert, unbefugte maliziöse Informationen (Schadcode, Angriffe) eingebracht werden können, die gezielt gegen diese Inspektions-Systeme oder die vor geschalteten Pass-Lesegeräte gerichtet sein können. Weiter könnten auch nach geordnete Systeme angegriffen werden.

2. Bei der BAC ist der Schlüssel zum Auslesen der Datengruppen DG.1 und DG.2 des RFID-Chips auf dem Dokument aufgedruckt. Somit sind die Informationen nicht gegen unbefugtes Auslesen gesichert (Information und Zugangscode sind auf demselben Medium gespeichert). Diese Informationen sind zudem in diversen nicht kontrollierbaren privatwirtschaftlichen Systemen zum Beispiel von Hotels, Mietwagenfirmen, Reisebüros, Geschäfte abgelegt.
   Durch diese Informationen sind eine unbemerkte Überwachung des MRTD-Inhabers sowie ein unberechtigtes Auslesen jederzeit möglich. Die Praxis, den Schlüssel aus der MRZ zu generieren, widerspricht sämtlichen Standards der Informationssicherheit.

3. Das dritte Risiko besteht darin, dass die Gültigkeit eines Zugriffsschlüssels nach EAC gegenüber dem Reisepass im Ausland nicht geprüft werden kann, da auf dem RFID-Chip kein Zeitnormal vorhanden ist und ein Rückrufmechanismus nicht existiert. Dieses steht konträr zu allen „Best-Practices“ von Public Key Infrastrukturen, die die Gültigkeit eines Schlüssels auch immer an Hand von Zeitstempeln prüfen und ebenfalls Rückrufmechanismen enthalten müssen. Dass wegen des fehlenden Zeitnormals statt dessen der Zeitstempel des Zertifikates zum Zeitpunkt des letzten berechtigten Auslesens im MRTD gespeichert ist, hilft nicht, diesen sicherheitstechnischen Mangel zu beheben. Im Gegenteil ermöglicht dies weitere Angriffe wie z.B. das automatische Entwerten der durch EAC geschützten MRTD-Daten durch einen falschen Zeitstempel. Außerdem bedeutet dies, dass in dem bisher nur lesbaren RFID-Chip im Reisepass jetzt auch nach dem ursprünglichen einmaligen Beschreiben der Information, welcher bis jetzt durch einen Schreibschutz manipulationsgesichert ist, immer wieder Informationen gespeichert werden müssen, was zwangsläufig weitere potenzielle Schwachstellen und Angriffspunkte mit sich bringt.

Zu § 6a Absatz (1) Datenübermittlung:

„Die Datenübertragung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und

Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden."

Hierzu muss angemerkt werden, dass nach dem aktuellen Stand der Technik bei dem Einsatz eines solchen Systems die Technologie nur einen kleinen Teil der Sicherheit darstellt.
Die organisatorischen Notwendigkeiten, wie regelmäßige Audits, das Absichern gegen Manipulationen an den Systemen für das entsprechende Verschlüsselungsverfahren, physischer Zugang und elektronischer Angriff, sowie die Sicherheitsorganisation und die regelmäßige Überprüfung, z.B. gegen Manipulation der Systeme bei den übermittelnden Stellen sowie der Vermittlungsstellen, sind im Gesetzentwurf nicht beachtet worden.

Der Sicherheitsstandard sollte vergleichbar zu dem Standard sein, der für die Systeme zum Übermitteln der Kundenstammdaten von den Banken an das BaFin bereits angewendet wird. Schließlich sollten die persönlichen biometrischen Daten des Bürgers mindestens genauso gut geschützt sein wie seine Kontonummern.

Zu §18 Abs.4 PassG

„Dabei kann alleine durch das Auslesen der maschinenlesbaren Zone weder auf das Lichtbild noch auf die Fingerabdrücke des Passinhabers zugegriffen werden."

Das ist nur bedingt gültig, da bei BAC der Schlüssel aus der maschinenlesbaren Zone generiert werden kann und somit die Daten ungeschützt jederzeit ausgelesen werden können. Bei EAC wird dafür zusätzlich noch ein weiterer Schlüssel benötigt, um auf die Fingerabdrücke zuzugreifen.

Durch das elektronische Speichern der MRZ für das API Verfahren besteht keinerlei Kontrolle über die durch das Verfahren abgelegten Daten. Mit Hilfe dieser Daten kann aber jederzeit das Bild ausgelesen werden oder durch einen reinen Lese-Versuch zwischen einem Reader und dem MRTD ist es möglich ein Bewegungsprofil zu erstellen.

Natürlich muss man nicht nur optisch die MRZ auslesen, sondern auch einen RFID-Reader einsetzen, um den gelesenen Schlüssel anzuwenden. Aber sobald die Daten der MRZ gelesen wurden, z.B. auf einer Fotokopie des Passes, gibt es keine Möglichkeit mehr, das Auslesen des Bildes zu verhindern oder zu bemerken. Da es in einigen Ländern gesetzlich vorgeschrieben ist, seinen Pass z.B. in Hotels abzugeben, besteht de facto keine Kontrolle darüber, wer die Daten der MRZ und damit den BAC-Schlüssel besitzen könnte. Ein Reisepass ist nun einmal zum Reisen in andere Länder vorgesehen – wenn er nur innerhalb Deutschlands „sicher" ist, reicht das naturgemäß nicht aus.
Auch Szenarien im Ausland müssen daher betrachtet werden.