Protokollauszug
aus der
40. öffentliche Sitzung des Ausschusses für Ordnung, Umweltschutz und Landwirtschaft
vom 24.01.2008

öffentlich

Top 3.7 Schutz von elektronischen Passdaten
07/SVV/1054
zur Kenntnis genommen

Herr Arndt bringt den Antrag ein und begründet diesen.

Frau Kluge informiert, dass der ePass in zwei Stufen von unberechtigtem Zugriff geschützt ist. Die erste Stufe BAC (Basic Access Control) wird bereits seit 2005 eingesetzt, um das Gesichtsbild und die biografischen Daten im ePass vor unberechtigtem Zugriff zu schützen. Die zweite Stufe EAC (Extended Access Control) wird seit 2007, zum zusätzlichen Schutz der Fingerabdruckdaten, eingesetzt.

Beim Zugriffsschutz BAC erhält ein Lesegerät vom Chip im ePass zunächst eine, eigens für den aktuellen Zugriff, generierte Zufallszahl zugeschickt. Mit dieser Zufallszahl und der im ePass abgedruckten MRZ (Maschine Readable Zone) kann das Lesegerät die Kommunikation aufbauen und die durch BAC geschützten Daten empfangen. Auf diese Weise wird einerseits sichergestellt, dass das Lesegerät physikalischen Zugriff auf den ePass hat (Kenntnis der MRZ) und andererseits, dass ein ePass ohne Kenntnis der MRZ nicht identifizierbar ist (Generierung einer Zufallszahl). Ein Angreifer könnte die durch BAC geschützten Daten im ePass also nur Auslesen, wenn er Zugriff auf diesen hat und erhält selbst dann nicht mehr Daten, als er durch das optische Ablesen der im ePass abgedruckten Daten erhält.

Da die Fingerabdrücke besonders sensitive Daten sind, werden sie zusätzlich durch den Zugriffsschutz EAC geschützt. Der Zugriffsschutz EAC basiert auf der gegenseitigen Authentisierung von Chip und Lesegerät durch eine gültige Zertifikatskette. Der Chip weist durch das in ihm gespeicherte Zertifikat gegenüber dem Lesegerät nach, dass er und die auf ihm hinterlegten Daten authentisch sind. Andersherum muss aber auch das Lesegerät, mit einer gültigen Zertifikatskette, welche vom Chip im ePass überprüft wird, nachweisen, dass es berechtigt ist auf die Fingerabdruckdaten zuzugreifen. Auf diese Weise wird sichergestellt, dass nur entsprechend autorisierte Lesegeräte vollen Zugriff auf die im Chip abgespeicherten Daten erhalten.

Zusätzlich zu den oben genannten Verfahren ist der Zugriff auch durch die physikalischen Eigenschaften des Chips und der Antenne stark eingeschränkt. Diese ermöglichen das aktive Auslesen des ePass lediglich im Abstand von maximal 20cm. Wobei dieser Maximalwert nur unter Laborbedingungen erreicht werden kann und ein Reichweite von 10cm bis 15cm unter Normalbedingungen realistisch ist.

Frau Kluge schlägt vor, im Bürgerservice die Adresse auszulegen, wo der Bürger die Schutzhüllen erhalten kann.

Herr Mühlberg hat herausgefunden, dass es so gut wie unmöglich ist, unter realen Bedingungen an die Daten heranzukommen.

Herr Walter weist darauf hin, dass dies als zusätzliche Sicherheitsmaßnahme gedacht ist.

Herr Arndt sieht den Antrag als durch Verwaltungshandeln erledigt und bittet, eine Information auf den Erwerb der Schutzhüllen im Bürgerservice.