erschien in: iX /10 (Oktober 2007) 48.

Der ePass -- innovativ, aber ein Sicherheitsrisiko

Ohne tiefergehende Analyse der Folgewirkungen seiner Einführung und unter Verweigerung einer breiten informierten Diskussion vor politischen Entscheidungen wurde der ePass in Deutschland eingeführt. Seine wesentlichen neuen Merkmale sind:

- ein Rechnerchip im Pass,

- alle Daten im Pass sind digital signiert,

- der Rechnerchip kommuniziert mit seiner Umwelt per Funk (RFID) und

- er enthält ein digitalisiertes Passbild sowie weitere biometrische Merkmale (nach aktuellem Stand Fingerabdruck).

Die Aufnahme eines Rechnerchips in den ePass bietet die Möglichkeit, wesentlich mehr Datenschutz zu realisieren, indem bei Kontrollen nicht einfach Passdaten ausgelesen (und potenziell unbegrenzt weiterverarbeitet) werden, sondern dem Rechnerchip das Ziel der Kontrolle mitgeteilt wird und dieser ausschließlich auf die damit verbundene(n) Frage(n) antwortet. Leider haben die Verantwortlichen diesen Vorteil der auch im Bundesdatenschutzgesetz geforderten Datenvermeidung/-sparsamkeit beim ePass-Konzept nicht berücksichtigt.

Das digitale Signieren aller Daten im Pass soll dessen Sicherheit gegen Manipulationen deutlich erhöhen. Damit haben Passfälscher als Angriffspunkt fast nur noch die ausstellende Behörde -- was immer diese an Daten für den Pass vorsieht, wird bei der Passproduktion sicher digital signiert. Wenn jedoch Pässe mit manipulierten Chips Lesegeräte zum Absturz bringen -- wie der Sicherheitsexperte Lukas Grunwald das bei der diesjährigen Black Hat demonstrierte -- nutzt auch das Vorhandensein signierter Daten nichts mehr.

Dass der Rechnerchip nicht kontaktbehaftet (wie etwa die Geldkarte) mit seiner Umwelt kommuniziert, sondern kontaktlos per Funk, kann man im günstigsten Fall als gedankenlose Dummheit bezeichnen. Funk ist deutlich leichter abzuhören als leitungsgebundene Kommunikation und der Rechnerchip im Pass ist gegen unerwünschte Kommunikationsversuche von außen deutlich schwerer zu schützen.

Zwar hat sich das BSI große Mühe gegeben, die daraus resultierende Unsicherheit durch kryptographische Protokolle halbwegs in den Griff zu bekommen. Aber es bleibt das Restproblem, dass der Rechnerchip seiner unsicheren Umgebung per Funk antwortet, diese Umgebung das Signal auswerten kann (ein Pass aus welchem Land oder gar ein Pass von welcher Person?) und damit ein Angreifer etwa nationalitäten- oder gar personenspezifische Reaktion auslösen kann -- beispielsweise das Zünden von Bomben. Die Argumentation des BMI und ihm untergeordneter Behörden, dass Bomben auch anders ausgelöst werden können, soll davon ablenken, dass die Kommunikation per Funk ein völlig unnötiges, zusätzliches Risiko verursacht -- ob es nun als relativ klein oder eher groß einzuschätzen ist.

Verantwortung abgewälzt

Die Aufbewahrung des ePasses in einem preiswerten Faradaykäfig (zu erhalten etwa bei Datenschutzbehörden), so dass jeglicher Funkkontakt mit der Umwelt und dadurch das nicht autorisierte Ansprechen des Passes unterbunden wird, ist
zwar eine Lösung, aber sie ist umständlich und erfordert Eigeninitiative des Bürgers. Dass das BMI die Lösung des Funkproblems auf die Bürger verschiebt, spricht nicht dafür, dass es bei der Einführung des ePasses um eine Steigerung ihrer Sicherheit geht.

Ab Herbst 2007 sollen in den deutschen ePass als biometrisches Merkmal auch die Fingerabdrücke des Inhabers aufgenommen werden. Durch das Prüfen der Fingerabdrücke bei jeder Passkontrolle werden die Bürger nach und nach daran gewöhnt, sie bereitwillig und ohne Nachzudenken an fremden Geräten (Fingerabdrucksensoren samt verbundener

IT) abzugeben. Zusammen mit ihrem Namen et cetera werden sie dann in zahllosen Geräten erfassbar: In solchen mit TÜV-Prüfung und Bundesadler mit hoffentlich eher geringem Missbrauchspotential, aber auch in Geräten anderer Länder, die in Bezug auf die Verwendung der erlangten Datensätze keinerlei gesetzlichen oder datenschutzrechtlichen Beschränkungen unterliegen.

Selbst wenn die vom BSI mitentwickelte Technik (extended access control) das Auslesen der Fingerabdruckreferenzmuster verhindert, erhält das Lesegerät Fingerabdrücke in hoher Qualität vom Sensor sowie aus dem ePass den Namen und weitere Daten des Inhabers. So können fremde Geheimdienste, auch von sogenannten Schurkenstaaten, sowie die organisierte Kriminalität ohne große Anstrengungen (oder gar notwendige Überzeugungsarbeit bei den Erfassten) umfangreiche Sammlungen von Fingerabdrücken samt Kontextdaten anlegen. Dies kann, je größer die Sammlung ist, desto gezielter zum Hinterlassen falscher, aber plausibler Fingerabdrücke an Tatorten sowie zur Enttarnung von Personen in Zeugenschutzprogrammen genutzt werden.

Dieses enorme Potenzial für organisierte Kriminelle und fremde Geheimdienste wird zum Alptraum für Polizei und Bürger -- also zum Gegenteil dessen, was intendiert war und von Ministerien und Behörden propagiert wurde. Die rechtzeitig erhobene Forderung, den deutschen ePass mit einer Anzeige auszustatten, ob dem Lesegerät der Zugriff auf die Fingerabdruckreferenzmuster erlaubt sein soll (dann mag es verantwortbar sein, seine Fingerabdrücke dort abzugeben) oder nicht (in dem Fall wäre Verweigerung und gegebenenfalls Verzicht auf Einreise angeraten), ignorierten die verantwortlichen Ministerien und Behörden.

In den vergangenen Jahren behaupteten selbst hohe Entscheidungsträger in Gesprächen über die Vor- und Nachteile des ePasses unter vier Ohren nach kurzem Austausch der Argumente nicht mehr, es ginge beim ePass um mehr Sicherheit. Es geht um die Förderung der deutschen IT- und Biometrieindustrie. Gegen diese Ziele ist nichts einzuwenden. Aber zum einen kann der Preis für die betroffenen Bürger unter Umständen sehr hoch

sein. Zum anderen darf man bezweifeln, dass das in jeder Hinsicht unzureichende Sicherheitskonzept dieses Produkt zu einem Exportschlager machen wird. Es dürfte im Gegenteil das Vertrauen in Sicherheitstechnik und insbesondere Biometrie untergraben. In Deutschland und anderswo. *Andreas Pfitzmann*

Weitere Argumente und Quellenhinweise finden sich unter www.inf.tu-dresden.de/index.php?node_id=703&ln=de. Zu den technischen und konzeptionellen Sicherheitsschwächen siehe auch Artikel "Sicherheitsbetrachtungen zum ePass: Vertrauensschwund" in *iX* 11/2006, S. 147-149.