Team 4 Innovation

„Neue Ausweise und Karten – es geht auch sicher!"
Systembeschreibung 4Security
(Stand 08/2006)

4Security ist eine patentierte Lösung zur manipulations- und fälschungssicheren Erfassung von biometrischen Daten:
- Preiswert in der Realisation,
- kostengünstig im Betrieb,
- sicher und effizient.

Analyse der Situation

Die Probleme bestehender Kartensysteme:

Bisherige Kartensysteme verfügen entweder über keine (Krankenkassenkarte) oder nur unzureichende Schutzmaßnahmen gegen unbefugte Benutzung.
4-stellige PIN-Nummern können den Missbrauch nicht wirklich ausschließen, zumal die PIN mit Hilfe des Kartencodes errechnet wird. Es gibt zwar mittlerweile EC-Karten, die durch einen auf der Karte aufgebrachten Chip angeblich fälschungssicher sind – dennoch hilft dies nicht gegen den Kartendiebstahl. Auch ein angeblich fälschungssicherer Chip kann dies nur auf Zeit sein, da diese Karten zu Millionen verbreitet sind und es keine Kontrolle über deren Verbleib gibt. Jeder kann diese Karten sammeln und die Chipstruktur in aller Ruhe analysieren. Nach seiner Analyse kann er aus dem Chip die notwendigen Daten zerstörungsfrei auslesen, denn der Chip muss auch dem Geldautomaten die notwendige Kennung übermitteln können.

Diese neuen EC-Karten sind demnach nicht wirklich sicherer, sie kosten jedoch das dreifache der alten Karten (laut Angabe der Sparkassen, die sich für deren Einsatz entschieden haben).

Bei der Gesundheitskarte versucht man durch ein Passbild bzw. durch auf der Karte vermerkte biometrische Daten Sicherheit zu erreichen.
All diesen Systemen bleibt das Problem, dass mehr oder weniger allgemein zugängliche Daten als Sicherheitsmerkmale eingesetzt werden und die beliebten 4-stelligen PINs derart unsicher sind, dass eher von „Unsicherheitssystemen" als von Sicherheitssystemen gesprochen werden kann:
Eine Chance von 1 zu 10.000 für die richtige PIN ist wahrlich kein Sicherheitsfaktor.

Die Lösung

4Security versucht nicht, Karten sicherer zu machen. Vielmehr wollen wir die Kartensicherheit indirekt durch ein **zentral gespeichertes** biometrisches Merkmal ergänzen. Denn – selbst wenn es nicht bemerkt wird, dass man seine Karte verliert, so wird man es eindeutig feststellen, wenn man seinen Finger verliert.
Ein Fingerabdruck ist etwas Einmaliges. Nicht umsonst ist er ein unumstrittenes gerichtsrelevantes Beweismittel. Man kann zwar einen Fingerabdruck abnehmen und kopieren, diese Kopien können jedoch durch eine schlichte Hautwiderstandsmessung aufgedeckt werden: Hierdurch können organische lebende Strukturen von anderen Strukturen unterschieden werden.

Dies alles ist jedoch nicht ausreichend, wenn man die derzeitige Anwendungsstruktur herkömmlicher Fingerprintscanner betrachtet. So wird bei herkömmlichen Systemen ein Bild erstellt und über den Rechner, an dem der Scanner angeschlossen ist, zu einer Zentralstelle übertragen oder gleich in diesem System verglichen. Der dort erzeugte Datenstrom kann jederzeit mitgeschrieben werden und somit – anstatt eines echten Fingerabdruckes – wieder verwendet werden.

Die Daten müssen vor jeglichem Missbrauch geschützt werden!

Das heißt: auch der Rechner hinter dem Scanner, das angeschlossene Netzwerk und alle anderen sich zwischen dem Scanner und dem Zentralsystem befindlichen Stellen müssen von der Nutzung ausgeschlossen werden. Eine normale Verschlüsselung würde beim selben Fingerprint wieder das selbe Muster erzeugen. Ein Mitschreiben und Wiederversenden wäre jederzeit möglich.

Unsere Lösung sorgt dafür, dass mitgeschriebene Daten absolut wertlos sind. Alternierende Keys – sowohl von der Zentrale als auch in der Fingerprint-scan- und Verschlüsselungseinheit – sorgen dafür, dass keine Mustererkennung stattfinden kann. Die hier übertragenen Daten könnten – theoretisch – selbst über das Internet ohne weitere Sicherungsmaßnahmen übertragen werden.
4Security erkennt und protokolliert jeden Manipulationsversuch.
Die Fingerprintdaten bekommen lediglich in der Zentrale wieder einen Wert.

Durch die ausschließliche Vermietung der Scanner und den Verbleib im Eigentum der Gesellschaft behält man die Übersicht über sämtliche Geräte. Ein weiteres Sicherheitsmerkmal kann die Forderung sein, dass mindestens einmal im Monat bei Nichtgebrauch eine Re-Identifizierung zu erfolgen hat. Erfolgt diese nicht, oder beendet ein Kunde seinen Vertrag, ist dieses Gerät an uns zurückzusenden. Auch ein Verlust ist umgehend zu melden; Weitergabe oder Verkauf bzw. ein Verschwinden dieser Geräte in dunklen Kanälen wird hiermit ausgeschlossen. Es ist zu überlegen, die Geräte an Personen zu binden; das heißt, selbst wenn solche Geräte in Firmen eingesetzt werden, gibt es Personen, die für den Verbleib des Gerätes persönlich haften und für die Folgeschäden im Falle eines Verlustes haftbar gemacht werden können. Auch sind diese Personen bei Manipulationsversuchen oder ähnlichem verantwortlich.

Das Prinzip dieser Lösung ist die Verlagerung der sicherheitsrelevanten Struktur weg von der Karte, hin zu Lesegeräten, die biometrische Daten aufnehmen und verschlüsselt übertragen. Die eigentlichen Daten finden sich hiermit nicht mehr zugänglich auf Karten, sondern in einem Zentralsystem. Dieses Zentralsystem ist mit einem gegebenen Aufwand viel leichter zu schützen als Millionen von Karten. Hier muss lediglich der Zugriff von außen über Datenleitungen geregelt werden. Ein Verlust dieses Systems und damit eine gewaltsame Strukturanalyse steht hingegen nicht zu befürchten.

Kosteneffizienter Einsatz

Für Banken:

Anstatt Millionen neuer Karten auszugeben, müssen bei einem solchen System nur die Bankautomaten und die Auszahlungsschalter nachgerüstet werden. Die Kosten hierfür halten sich im Rahmen.
Weiterer Nachrüstungsbedarf besteht im Einzelhandel. Auch besteht die Möglichkeit, dieses System anstatt von HBCI einzusetzen. Diese Kosten träfen dann aber nicht mehr die Banken.

Für den öffentlichen Bereich:

Für Finanzbehörden und weitere E-Government Systeme wäre eine Fingerabdruckkartei vonnöten, die man für den biometrischen Personalausweis ohnehin anlegen muss. Die eigentlichen Geräte benötigt der Bürger ebenfalls, beispielsweise für Bankgeschäfte. Es wären also sichere E-Government Lösungen zu minimalen Kosten möglich; der Datenschutz wäre hierbei auch gewährleistet.

Für das Gesundheitswesen:

Sichere Patientenerkennung ohne teure Karten. Höchstes Sicherheitsniveau bei geringsten Kosten. Es wird lediglich das Zentralsystem benötigt. Die sonstigen

Kosten könnten sogar von den Ärzten getragen werden. Bedenkt man den Kostenunterschied zu einer Gesundheitskarte, so wären die Kosten für die Erfassungsgeräte im Vergleich dazu nur marginal.

Für e-commerce Plattformen (wie ebay, webshops, etc.):

Das System kann zusammen mit der Identifizierung durch ein Zentralsystem – als Service durch die Banken etwa – die Identität einer Person zweifelsfrei nachweisen. Betrug würde hierdurch de facto ausgeschlossen. Eine Willenserklärung wäre hiermit eindeutig nachweisbar und zuordenbar. Es kann im Streitfall sogar nachvollzogen werden, von welchem Gerät aus diese erfolgt ist.

Zusammenfassung

Dieses zum Patent angemeldete System kann die Basis für funktionierende elektronische Banking-, Bezahl- und Leistungssysteme werden.
Bei einer überschaubaren Investition ist maximale Sicherheit gewährleistet. Diese geht so weit, dass sogar Manipulations**versuche** aufgezeichnet und damit verfolgbar gemacht werden.
Auf Grund der bestechenden Preis/Leistungsrelation ist 4Security ein Gewinn für die gesamte Volkswirtschaft.

Gerne stehen wir für Fragen zur Verfügung:

Team 4 Innovation GBR
Axel Ahnert, Technische Leitung
Herbststr. 27
D-85737 Ismaning
Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
E-Mail: info@team4innovation.com