On-Card-Matching handschriftlicher Unterschriften auf elektronischen Signaturkarten (Extended Abstract)

Dr.-Ing. Olaf Henniger
Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstr. 75, 64295 Darmstadt
olaf.henniger@sit.fraunhofer.de

1 Motivation

Damit die Mittel zur Erzeugung elektronischer Signaturen unter der alleinigen Kontrolle der jeweiligen rechtmäßigen Signaturschlüsselinhaber gehalten werden können, werden zur sicheren Aufbewahrung privater Signaturschlüssel und als geschützte Umgebung für die Erzeugung elektronischer Signaturen oft manipulationsgeschützte, personengebundene Smartcards (Chipkarten mit Mikroprozessorchip) eingesetzt [Pie04, prEN 14890-1].

Zur Prüfung der Zugriffsberechtigung auf die geschützten Funktionen einer Signaturkarte können zusätzlich oder als Alternative zur üblichen Abfrage einer geheimen PIN (Personal Identification Number) auch biometrische Verifikationsverfahren eingesetzt werden. Dabei erfolgt ein Eins-zu-eins-Vergleich der biometrischen Merkmale des aktuellen Karteninhabers mit den zuvor beim „Enrollment“ als Referenzdaten in der Smartcard abgespeicherten biometrischen Merkmalen des rechtmäßigen Karteninhabers, um festzustellen, ob der aktuelle Karteninhaber der rechtmäßige ist, und gegebenenfalls den Zugriff auf die geschützten Funktionen freizugeben.

Biometrische Verfahren werden oft als benutzerfreundlicher empfunden, als aus dem Gedächtnis eine 6stellige PIN einzutippen, besonders wenn diese zufällig gewählt ist. Man stelle sich z. B. einen Arzt vor, der elektronische Rezepte mit der Signierfunktion seines Heilberufsausweises signieren soll. Da biometrische Merkmale an eine bestimmte Person gebunden sind, können biometrische Benutzerauthentisierungsverfahren auch die Bindung elektronischer Signaturen an den rechtmäßigen Signaturschlüsselinhaber verstärken, wenn die Überwindungssicherheit und Erkennungsleistung der biometrischen Verfahren ausreichend hoch sind. Da handschriftliche Unterschriften seit langem als Mittel zur Authentisierung akzeptiert sind und als Ausdruck einer willentlichen Entscheidung des Schreibers angesehen werden, sind Unterschriftserkennungsverfahren im Zusammenhang mit elektronischen Signaturen besonders vielversprechend.

Damit der Smartcard mit der zu schützenden Signierfunktion ein positives Verifikationsergebnis nicht vorgetäuscht werden kann, erfolgt beim On-Card-Matching der Vergleich der Verifikations- und Referenzdaten in der Smartcard selbst. On-Card-Matching bietet zusätzlich den Vorteil, daß die biometrischen Referenzdaten des rechtmäßigen Karteninhabers nie aus der Smartcard ausgelesen werden und damit vor Mißbrauch geschützt bleiben, falls die Karte in die Hände Unbefugter gelangt.

2 Umsetzung

Die heutigen Smartcard-Controller sind leistungsfähig genug für den Vergleich biometrischer Merkmale, auch wenn ihre Rechenleistung und Speicherkapazität im Vergleich zu der von PCs deutlich eingeschränkt ist. Die meisten bisher verfügbaren On-Card-Matching-Implementierungen sind Fingerabdruckvergleichsverfahren. Am Fraunhofer-Institut für Sichere Informationstechnologie wurde jedoch auch On-Card-Matching für handschriftliche Unterschriften prototypisch auf der Basis von Java-Karten implementiert. Es werden vorverarbeitete Unterschriftszeitreihen in einem kompakten Binärformat nach [ISO/IEC 19794-7] mittels Dynamic-Time-Warping verglichen [HF04]. Zur Verbesserung der Benutzerfreundlichkeit muß vor allem noch die benötigte Rechenzeit verringert werden. Dies läßt sich erreichen, wenn der Unterschriftsvergleich anstatt in Java in Maschinenkode des Smartcard-Controllers ausgeführt wird.

Der On-Card-Matching-Algorithmus für handschriftliche Unterschriften wurde in OpenPGP-Karten integriert, die im Zusammenspiel mit OpenPGP-Software auf dem PC zum Signieren und Entschlüsseln von Nachrichten eingesetzt werden können.

Obwohl biometrische Benutzerauthentisierungsverfahren oftmals als benutzerfreundlicher als die Eingabe einer PIN empfunden werden und obwohl sie das Potential besitzen, die Bindung von elektronischen Signaturen an die Person zu verbessern, kommen biometrische Verfahren in Europa bisher nur kaum bei der Erzeugung qualifizierter elektronischer Signaturen (mit denen wie mit einer handschriftlichen Unterschrift rechtsverbindliche Erklärungen abgegeben werden können) zum Einsatz. Ein Grund dafür ist, daß die durch gesetzliche Verordnungen geforderten Sicherheitszertifikate nach anerkannten Evaluierungsverfahren wie den Common Criteria für biometrische Produkte noch nicht vorliegen. Der für die Evaluierung erforderliche Vergleich der Sicherheit von biometrischen Benutzerauthentisierungsverfahren mit der Sicherheit der PIN stellt noch ein offenes Problem dar.

Literatur

[HF04] O. Henniger, K. Franke: Biometric User Authentication on Smart Cards by Means of Handwritten Signatures. In D. Zhang, A.K. Jain (Hrsg.): *Proceedings of the 1st International Conference on Biometric Authentication*, Hong Kong, China, 2004. Springer (Lecture Notes in Computer Science, Vol. 3072)

[ISO/IEC 19794-7] Final Draft International Standard ISO/IEC 19794-7:2007, Information Technology – Biometric Data Interchange Formats – Part 7: Signature/Sign Time Series Data

[Pie04] A. Pietig: Functional Specification of the OpenPGP Application on ISO Smart Card Operating Systems. Version 1.1, 2004

[prEN 14890-1] Draft European Standard prEN 14890-1:2007, Application Interface for Smart Cards Used as Secure Signature Creation Devices – Part 1: Basic Services,