OpenPGP-Karten mit biometrischer Benutzerauthentisierung

Jan Trukenmüller, Olaf Henniger

{jan.trukenmueller | olaf.henniger}@sit.fraunhofer.de

Zusammenfassung: OpenPGP-Karten sind Smartcards, die private OpenPGP-Schlüssel sicher speichern und Entschlüsselungs- und Signierfunktionen bereitstellen. Der Benutzer einer OpenPGP-Karte muss sich gegenüber der Karte authentisieren. Dieser Beitrag beschreibt die prototypische Implementierung von OpenPGP-Karten mit biometrischem On-Card-Matching. Außerdem wird die Integration der Komponenten zur Erfassung und Verarbeitung biometrischer Daten in eine OpenPGP-basierte E-Mail-Anwendung beschrieben. Als Methoden zur Benutzerauthentisierung werden neben Passwörtern Fingerabdrücke und handgeschriebene Unterschriften unterstützt.

1 Stand der Technik

1.1 E-Mails und Kryptographie

Sollen vertrauliche Informationen mit Hilfe von E-Mails versendet werden, so ist es empfehlenswert, diese zu verschlüsseln. Um die Identität des Absenders zu beweisen, können digitale Signaturen verwendet werden. Diese stellen gleichzeitig sicher, dass Manipulationen an einer Nachricht auf dem Weg zum Empfänger entdeckt werden können. Für die E-Mail-Kryptographie haben sich S/MIME [DHR+98] und OpenPGP [CDFT98] als Standards etabliert. Beide machen von asymmetrischen kryptographischen Verfahren Gebrauch. Dabei werden Schlüsselpaare mit jeweils einem öffentlichen und einem privaten Schlüssel verwendet. Die Geheimhaltung des privaten Schlüssels ist für die Sicherheit von Verschlüsselung und digitaler Signatur von entscheidender Bedeutung.

1.2 Smartcards als persönliche Sicherheitsumgebungen

Idealerweise werden private Schlüssel innerhalb einer persönlichen Sicherheitsumgebung (PSU) erzeugt und aufbewahrt und verlassen diese zu keiner Zeit. Sämtliche Algorithmen, die auf private Schlüssel zugreifen, müssen in der PSU ausgeführt werden. Die PSU bietet lediglich Schnittstellen nach außen, über die diese Algorithmen aufgerufen werden können. Dabei muss sie dafür sorgen, dass nur der berechtigte Eigentümer die Funktionen zum Entschlüsseln oder Signieren aufrufen kann.

Für die Realisierung einer PSU sind Smartcards geeignet. Das sind manipulationsgeschützte Chipkarten mit integrierten Mikroprozessoren, also mit der Fähigkeit zur programmgesteuerten Datenverarbeitung direkt auf der Karte.

Speziell für die Realisierung einer OpenPGP-PSU wurde die OpenPGP-Karte [Pie04a] spezifiziert. Diese Smartcard speichert die privaten Schlüssel zum Signieren und Entschlüsseln und kann die erforderlichen kryptographischen Algorithmen ausführen. Außerdem ist sie in der Lage, neue Schlüsselpaare zu erzeugen. Um sicherzustellen, dass die Karte nur vom berechtigten Eigentümer benutzt werden kann, ist in der Spezifikation die Verwendung von alphanumerischen Kennwörtern vorgesehen. Bisher gibt es nur eine Implementierung der OpenPGP-Anwendung auf BasicCards [Pie04b, Sal05].

1.3 Biometrische Benutzerauthentisierung

Als Identitätsnachweis kommen alternativ zu Passwörtern auch biometrische Verfahren in Frage. Dabei werden biometrische Merkmale erfasst und mit zuvor gespeicherten Referenzmerkmalen des berechtigten Eigentümers verglichen. Sind die Merkmale ähnlich genug, so ist der Benutzer authentisiert.

Soll ein biometrisches Verfahren als Identitätsnachweis gegenüber einer PSU benutzt werden, so muss die PSU die biometrischen Referenzmerkmale speichern und den Vergleich durchführen. Ansonsten könnte ihr eine positive Authentisierung vorgetäuscht werden.

Am Fraunhofer-Institut SIT wurde eine Lösung zum On-Card-Vergleich von handgeschriebenen Unterschriften entwickelt [HF04]. Diese Anwendung wurde auf Java-Karten programmiert, also Smartcards, die in Java geschriebene Karten-Applets interpretieren. Ein Java-Card-Applet zum Erkennen von Fingerabdrücken gibt es z. B. von der Firma Precise Biometrics: „Precise BioMatch J“ [NH04].

Um auf Java-Karten die biometrische Authentisierungsmethode einfach austauschen zu können, wurde die Java Card Biometric API [BC02] spezifiziert. Voraussetzung für einen reibungslosen Austausch der biometrischen Komponenten ist, dass diese Schnittstelle sowohl vom Authentisierungs-Applet als auch vom Anwendungs-Applet unterstützt wird. Das Applet „Precise BioMatch J“ unterstützt die Java Card Biometric API.

2 OpenPGP-Anwendung mit biometrischem On-Card-Matching

2.1 Überblick

Es wurde eine OpenPGP-Karte mit biometrischem On-Card-Matching entwickelt [Aza06]. Außerdem wurden die zur Benutzung dieser Karte erforderlichen Komponenten zur Erfassung und Verarbeitung biometrischer Daten in die OpenPGP-Software auf dem PC integriert [Tru06]. Insgesamt waren folgende Schritte notwendig:

- Entwicklung eines OpenPGP-Java-Card-Applets, das die Java Card Biometric API als Schnittstelle zu Authentisierungs-Applets benutzt;
- Integration biometrischer Authentisierungs-Applets in die Karte und Entwicklung eines Programms zum Personalisieren dieser Applets;
- Anpassen eines E-Mail-Clients an die biometrischen Authentisierungsmethoden.

2.2 OpenPGP-Karte

Als Implementierungsplattform dienen Java-Karten, die die von OpenPGP benötigten kryptographischen Funktionen über die Java-Card-API [JCA00] zur Verfügung stellen.

Das OpenPGP-Applet ist gemäß [Pie04a] programmiert. Die wichtigsten Kartenkommandos, die es bietet, sind PSO (PERFORM SECURITY OPERATION):COMPUTE DIGITAL SIGNATURE zum Berechnen digitaler Signaturen und PSO:DECIPHER zum Entschlüsseln. [Pie04a] sieht drei Passwörter (CHV1, CHV2 und CHV3) als Referenzdaten zum Authentisieren vor. CHV1 muss vor dem Ausführen des Kommandos PSO:COMPUTE DIGITAL SIGNATURE authentisiert werden. Die Authentisierung von CHV2 ermöglicht das Ausführen von PSO:DECIPHER. Um administrative Kommandos verwenden zu können, muss CHV3 authentisiert werden.

Die OpenPGP-Karte unterstützt die Java Card Biometric API, um neben einer Passwort-Authentisierung auch die Authentisierung durch einen Fingerabdruck oder eine handgeschriebene Unterschrift zu ermöglichen. Die Referenzdaten und Methoden zum Authentisieren wurden in Objekten gekapselt, die über die Java Card Biometric API mit dem OpenPGP-Applet kommunizieren.

Die biometrischen Applets müssen personalisiert werden, bevor man sie verwenden kann. Dafür wurde ein Personalisierungsprogramm entwickelt. Mit diesem können die Template-Container mit Referenzdaten gefüllt werden.

2.3 Demonstrationsprototyp für E-Mail-Kryptographie

Als Basis für den Demonstrationsprototypen dient der E-Mail-Client „Mozilla Thunderbird“. Die OpenPGP-Erweiterung „Enigmail“ für diesen Client unterstützt auch OpenPGP-Karten. Enigmail verwendet wiederum das Programm GnuPG, welches die Zugriffe auf die Karte durchführt und die kryptographischen Funktionen bereitstellt.

Die OpenPGP-Software wurde so modifiziert, dass neben einer Benutzerauthentisierung mit Passwörtern auch biometrische Verfahren möglich sind. Das bedeutet, dass folgende zusätzliche Funktionen unterstützt werden:

- **Auswahl des Authentisierungsverfahrens** – Dies ist nötig, damit der Benutzer zwischen Passwort, Fingerabdruck und handgeschriebener Unterschrift wählen kann. Hierfür wurde die graphische Oberfläche von Enigmail angepasst.

- **Erfassung von Fingerabdrücken und Unterschriften** – Dies beinhaltet den Zugriff auf den Fingerabdruck-Sensor bzw. das Graphik-Tablett, die Anzeige von Fingerbild bzw. Unterschrift am Bildschirm als Rückmeldung für den Benutzer und die Extraktion von Merkmalen aus den erfassten biometrischen Daten.
- **Senden biometrischer Daten an die Karte** – Sowohl zum Authentisieren als auch zum Ändern der Referenzdaten müssen die Merkmalsdaten eines Fingerabdrucks oder einer Unterschrift an die OpenPGP-Karte gesendet werden.

Für den Kartenzugriff wurde ein Wrapper um den PC/SC-Resource-Manager [PCS04] programmiert. Der Wrapper greift nach unten auf den PC/SC-Resource-Manager zu und bietet als obere Schnittstelle die CT-API [MKT99]. Der Wrapper kann in GnuPG und Enigmail als Treiber für den Kartenleser eingebunden werden. Er fängt alle Kartenkommandos zum Prüfen oder Ändern der Passwörter ab, sorgt für die Erfassung der gewählten biometrischen Daten und sendet diese zur Karte. Kommandos ohne Passwort werden unverändert an die Karte weitergeleitet. Abbildung 1 verdeutlicht diese Zusammenhänge.

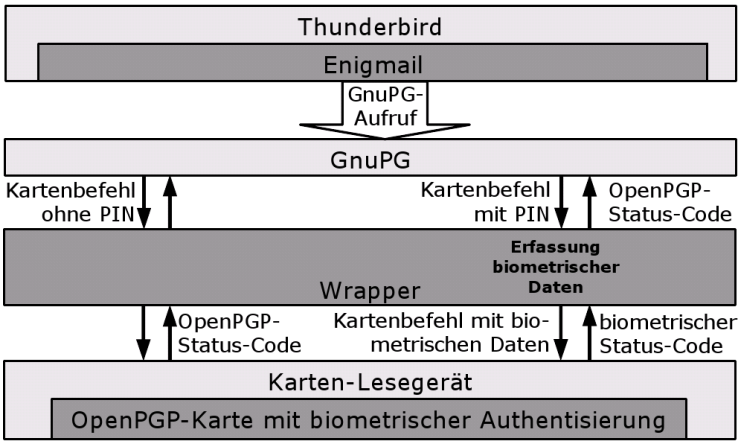

Abbildung 1: Architektur des Kartenzugriffs

3 Zusammenfassung und Ausblick

Biometrische Authentisierungsverfahren bieten mit ihrer relativ einfachen Benutzbarkeit und der starken Bindung des Identitätsnachweises an die Person Vorteile für den Anwender. Die vorgestellte prototypische Entwicklung zeigt die Machbarkeit von E-Mail-Kryptographie unter Verwendung einer Smartcard mit biometrischem On-Card-Matching als PSU. Es wurde eine auf Java-Karten lauffähige OpenPGP-Anwendung entwickelt, die zur Authentisierung auf die Java Card Biometric API aufsetzt. Dadurch können verschiedene biometrische On-Card-Matching-Technologien zur Authentisierung verwendet werden.

Die zur Erfassung, Vorverarbeitung und Formatierung von Fingerabdrücken und Unterschriftsdaten erforderlichen Komponenten wurden in Form eines Wrappers für den PC/SC-Resource-Manager in das OpenPGP-Programm auf dem PC integriert. Da der Wrapper dem aufrufenden Programm die Schnittstelle eines Kartenterminal-Treibers zur Verfügung stellt, kann er auch von anderen Anwendungen wiederverwendet werden, die Smartcards mit biometrischer Benutzerauthentisierung unterstützen.

Danksagung

Unser Dank gilt Frau Marina Azarhoush für ihren Anteil an der vorgestellten Entwicklung.

Literatur

[Aza06] M. Azarhoush. *Implementierung einer OpenPGP-Karte mit biometrischem On-Card-Matching*. Diplomarbeit, Hochschule Mannheim, 2006.

[BC02] Java Card Biometric API. White paper, Biometric Consortium, 2002.

[CDFT98] J. Callas, L. Donnerhacke, H. Finney und R. Thayer. OpenPGP Message Format. Network Working Group Request for Comments 2440, 1998.

[DHR+98] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade und L. Repka. S/MIME Version 2 Message Specification. Network Working Group Request for Comments 2311, 1998.

[HF04] O. Henniger und K. Franke. Biometric user authentication on smart cards by means of handwritten signatures. In D. Zhang und A.K. Jain, Hrsg., *1st International Conference on Biometric Authentication*, Hong Kong, China, 2004.

[JCA00] Java Card 2.1.1 Application Programming Interface. Sun Microsystems, 2000.

[MKT99] Multifunktionale Kartenterminals (MKT) für das Gesundheitswesen und andere Anwendungsgebiete – Teil 3: CT-API 1.1 – Anwendungsunabhängiges Card-Terminal Application Programming Interface. TeleTrusT Deutschland e.V., 1999.

[NH04] J. Nilsson und M. Harris. Match-on-Card for Java Cards. White paper, Precise Biometrics, 2004.

[PCS04] Interoperability Specification for ICCs and Personal Computer Systems – Part 5: ICC Resource Manager Definition. PC/SC Workgroup, 2004.

[Pie04a] A. Pietig. Functional Specification of the OpenPGP Application on ISO Smart Card Operating Systems, 2004.

[Pie04b] A. Pietig. OpenPGP-Smartcard – Die Signaturkarte für Jedermann. In B. Struif, Hrsg., *14. SIT-Smartcard-Workshop*, Darmstadt, 2004.

[Sal05] W. Salge. Smart Card Basics oder BASIC for Smart Cards. In B. Struif, Hrsg., *15. SIT-Smartcard-Workshop*, Darmstadt, 2005.

[Tru06] J. Trukenmüller. *Integration von OpenPGP-Karten mit biometrischer Benutzerauthentisierung in einen E-Mail-Client*. Diplomarbeit, Berufsakademie Mannheim, 2006.