PDA+CC Crypto-Library

Zu entwickeln ist eine „Java PDA+CC Crypto-Library“, die es dem Programmierer von PDA-Anwendungen erlaubt, sensitive Daten auf die Chipkarte auszulagern, bzw. sicherheitskritische Funktionen auf der Chipkarte auszuführen. Die Nutzung der Chipkarte soll dabei für Programmierer und Benutzer der Anwendung völlig transparent sein.

Die Funktionalität wird zwischen PDA und Chipkarte folgendermaßen aufgeteilt:

- Auslagerung der sicherheitskritischen Funktionen auf die Chipkarte:
  - Speicherung von Schlüsseln, Zertifikaten und anderen sensiblen Daten
  - Signaturerstellung und Verifikation
- Rechenintensive Funktionen verbleiben am PDA:
  - Hashen
  - Schlüsselgenerierung
  - Ver- und Entschlüsseln

Wichtig: Geheime Schlüssel sollten möglichst kurz im Speicher des PDAs verweilen! Wird am PDA z.B. die Verschlüsselung von Daten verwendet, so wird zuerst der Benutzer zur Eingabe der PIN aufgefordert. Die eingelesene PIN wird auf der Chipkarte verifiziert und anschließend kann der gewünschte Schlüssel ausgelesen werden. Nach Verwendung des Schlüssels am PDA wird dieser sofort gelöscht.

Das Modul zur Kommunikation mit der Chipkarte ist bereits vollständig vorhanden, die im Rahmen der Kommunikation eingesetzten APDUs (Application Protocol Data Units) sind in Grundzügen vorhanden. Die relevanten Methoden der Chipkarte sind ebenfalls teilweise vorhanden.

Möglicher Funktionsumfang:

- Sicherer Datenspeicher
- Sicherer Zähler
- Sicheres Log-File
- Generierung von Pseudozufallszahlen
- Schlüsselmanagement (Generierung und Verwaltung)
- Ver- und Entschlüsselung (symmetrisch und asymmetrisch)
- Signaturerstellung und Verifikation

Voraussetzungen:

- Fundierte Kenntnisse der Programmiersprache Java (PDA und Chipkarten werden mittels Java bzw. JavaCard programmiert)
- Grundkenntnisse der Systemsicherheit (z.B. VO Systemsicherheit)
- Grundkenntnisse der PDA- und Chipkarten-Programmierung (z.B. PDA- & CC-Labor)

Teilnehmer:
2 Studierende Informatik

Ansprechpartner:
Dr. Peter Schartner (E.1.51, DW 3718, e-Mail: peter.schartner@uni-klu.ac.at)