

Abschlussbericht für das Modul SmartCard-Programmerung

Implementierung einer Multicard-Anwendung

29. August 2016

Inhaltsverzeichnis

1	Einleitung	3
2	Oncard	4
2.1	Student-Applet	5
2.1.1	Geld	6
2.1.2	Studentendaten	7
2.1.3	Raumfreischaltung	8
2.2	Disco-Applet	8
2.2.1	Bonus	9
2.2.2	Geld	10
2.2.3	Getränke	10
2.3	Crypto-Applet	11
2.3.1	Funktionsweise	11
2.3.2	Verschlüsselung	14
2.3.3	Entschlüsselung	14
3	OffCard	15
3.1	Simulation	15
3.2	Connection-Tab	15
3.3	Configuration-Tab	15
3.4	Student-Tab	15
3.5	Disco-Tab	15
4	Fazit	15

1 Einleitung

In dem Projekt „Implementierung einer MultiCard“ für das Wahlpflichtmodul „SmartCard-Programmierung“ im Sommersemester 2016 geht es um eine beispielhafte Realisierung einer SmartCard-Anwendung. Zu einer SmartCard-Anwendung gehören sogenannte On- und OffCard-Teile. Der OnCard-Teil beschreibt die Anwendung auf der SmartCard, während der OffCard-Teil die Nutzerseite beschreibt.

In dem Projekt „Implementierung einer MultiCard“ sollen mögliche Anwendungen für eine Studenten- und Discokarte realisiert werden. Gleichmaßen soll jegliche Kommunikation kryptographisch verschlüsselt erfolgen, damit eine Manipulation der Karte beziehungsweise der Daten auf der Karte verhindert werden.

Aufgabe: Es sollte eine SmartCard-Anwendung entstehen, welche als Bestandteile zum Einen eine Studenten-Karte realisiert. Zum Anderen soll die SmartCard eine sogenannte Disco-Karte realisieren. Weiterhin soll die komplette Kommunikation verschlüsselt erfolgen.

Bestandteile der Student-Anwendung sind:

- Studentenname und Matrikel
- Raumzugänge
- Geld einzahlen und per Essen verbrauchen
- Daten abfragen

Bestandteile der Disco-Anwendung sind:

- Geld einzahlen
- Konsumierte Getränke speichern und bezahlen
- Bonuspunkte für Konsum und verbrauchen der Punkte
- Daten abfragen

Bestandteile der Kryptographie sind:

- Verschlüsseln
- Entschlüsseln
- Signierung

Verlauf: Im Verlauf des Projektes wurden die Anforderungen entsprechend der Aufgabe realisiert. Das gesamte Projekt wurde per sogenanntem „Pair-Programming“ realisiert. „Pair-Programming“ bezeichnet das gemeinsame Programmieren an einem Bildschirm, während einer das Programm schreibt denkt der jeweils andere über das geschriebene nach. Regelmäßig werden diese beiden Rollen getauscht.

Aufgrund dass unter Linux programmiert wurde, kann die realisierte Anwendung nicht real getestet werden, da benötigte Treiber nicht existieren. Daher wurde das gesamte Projekt in der Simulation getestet.

Ergebnis: Als Ergebnis des Projektes entstand eine kryptographisch gesicherte SmartCard-Anwendung, welche ein Studenten-, Disco- und Crypto-Applet enthält. Außerdem entstand eine OffCard-Anwendung welche diese Funktionalitäten der SmartCard anspricht. Der Einfachheit halber wurde die OffCard-Anwendung in Tabs untergliedern um die verschiedenen Einsatzbereiche abzutrennen.

Aufbau: In diesem Bericht wird zunächst auf die verschiedenen Applets mit Ihren Anweisungen und den verschiedenen Fehlern eingegangen. Im Anschluss an den OnCard-Teil wird auf den OffCard-Teil eingegangen. Am Ende des Berichtes wird ein Fazit über das realisierte Projekte gezogen.

2 Oncard

Innerhalb der Applets auf der SmartCard wurden zum Teil eigene Fehler definiert. Dies erleichtert die Lokalisierung von Fehlern und Problemen bei der Abarbeitung von Anweisungen auf der SmartCard. Falls ein Fehler auftritt, wird dieser an die OffCard-Anwendung weitergeleitet und entsprechend behandelt. Die selbst

definierten Fehler-Codes werden nachfolgend bei den entsprechenden Applets angegeben.

Zu den selbst definierten Fehler-Codes können noch folgende allgemeine Fehler auftreten:

- ISO7816.SW_CLA_NOT_SUPPORTED
 - Klassenbyte wird nicht unterstützt.
- ISO7816.SW_INS_NOT_SUPPORTED
 - Anweisung wird nicht unterstützt.
- ISO7816.SW_WRONG_LENGTH
 - Daten haben falsche Länge.
- ISO7816.SW_DATA_INVALID
 - Daten sind ungültig (wurden manipuliert).

Der OnCard-Teil enthält die drei Applets: Student, Disco und Crypto.

2.1 Student-Applet

Die AID des Student-Applets ist Student in hexadezimal geschrieben:

- 0x 53 74 75 64 65 6e 74

Das Klassenbyte für das Student-Applet ist:

- 0x 20

Das Student-Applet unterteilt sich in drei Komponenten. Zum Einen die Funktionalität mit Geld umzugehen und zum Anderen das Speichern von Studentennamen sowie die Raumfreischaltungen. Das Essen in der Mensa auf der Studentenkarte wird durch einfaches Geld ausgeben realisiert.

2.1.1 Geld

Im Student-Applet kann Geld eingezahlt und verbraucht werden, dabei wird Euro und Cent jeweils als 1 Byte dargestellt. Auf der Karte wird zwischen ganzzahligem Euro-Betrag und Cent-Betrag unterschieden. Daraus ergibt sich für den Euro-Betrag eine Obergrenze von 127€, da sonst ein Überlauf des Bytes erfolgen würde. Die Höchstgrenze für den Cent-Betrag ist auf 99¢ gesetzt. Sodass der Höchstbetrag auf der Karte 127,99€ ist.

INS_GET_MONEY (0x20) Liefert das aktuell auf der Karte gespeicherte Guthaben.

INS_ADD_MONEY (0x21) Fügt der Karte Geld hinzu.

Folgende Fehler können geworfen werden:

- **ERROR_ADD_EURO_OVERFLOW (0xE021)**
 - Es kann kein ganzzahliger Betrag mehr hinzugefügt werden, da sonst ein Überlauf entstehen würde.
- **ERROR_ADD_CENT_OVERFLOW (0xE121)**
 - Bei dem hinzufügen von Cents, entsteht ein Überlauf im Euro.
- **ERROR_ADD_MONEY_OVERFLOW (0xE221)**
 - Hinzufügen von Euro und Cent sorgt für einen Überlauf.

INS_SUB_MONEY (0x22) Es wird ein Betrag vom Geld subtrahiert und damit ausgegeben.

Folgende Fehler können geworfen werden:

- **ERROR_SUB_EURO_UNDERFLOW (0xE022)**
 - Subtraktion von Euro führt zu einem Unterlauf des Guthabens.

- **ERROR_SUB_CENT_UNDERFLOW (0xE122)**
 - Subtraktion von Cents führt zu einem Unterlauf des Guthabens.
- **ERROR_SUB_INSUFFICIENT_MONEY (0xE222)**
 - Nicht genügend Guthaben auf der Karte.

INS_RESET_MONEY (0x23) Setzt Euro- und Cent-Betrag auf der Karte auf Null (Werkszustand).

2.1.2 Studentendaten

Auf der Karte wird der Name sowie die Matrikelnummer des Studenten gespeichert.

INS_SET_NAME (0x24) Schreibt den Namen des Studenten auf die Karte. Der Name des Studenten darf maximal 50 Zeichen lang sein.

INS_GET_NAME (0x25) Liefert den gespeicherten Namen.

INS_SET_MATRIKEL (0x26) Setzt die Matrikelnummer des Studenten als Zahl (2 Byte). Die Matrikelnummer darf höchstens 32767.

Folgende Fehler können geworfen werden:

- **ERROR_SET_MATRIKEL_NEGATIVE (0xE025)**
 - Matrikelnummer darf nicht negativ sein.
- **ERROR_SET_MATRIKEL_OVERFLOW (0xE125)**
 - Matrikel ist größer als höchstmöglicher Wert, wodurch ein Überlauf entstehen kann.

INS_GET_MATRIKEL (0x27) Liefert die gespeicherte Matrikelnummer des Studenten.

2.1.3 Raumfreischaltung

Räume für den Studenten werden freigeschaltet in dem geprüft wird ob der Raum auf der SmartCard gespeichert ist (in Anlehnung an das System der HTWK Leipzig). Damit Räume freigeschaltet werden können, werden diese als Liste auf der Karte gespeichert. Es wird dabei immer die komplette Liste gesetzt beziehungsweise abgefragt. Auf der Karte können maximal 16 Räume gespeichert werden. Jeder Raum besteht aus drei Bytes (Buchstaben + Nummer).

INS_SET_ROOMS (0x28) Speichert die als Liste übergebenen Räume auf der Karte.

INS_GET_ROOMS (0x29) Liefert eine Liste von gespeicherten Räumen auf der Karte

2.2 Disco-Applet

Die AID des Disco-Applets ist Disco in hexadezimal geschrieben:

- 0x 44 69 73 63 6f

Das Klassenbyte für das Disco-Applet ist:

- 0x 30

Das Disco-Applet besteht im Wesentlichen aus drei Komponenten. Zum Einen das Sparen von Bonuspunkten durch Konsum von Getränken sowie das Speichern der verbrauchten Getränke auf der Karte. Zum Anderen müssen die Getränke mit Hilfe von Geld (aus Student-Applet) und Bonuspunkten bezahlt werden. Üblicherweise wird die SmartCard bei Betreten der Lokalität vorgelegt und der Eintritt bezahlt.

Beim Verlassen der Lokalität wird die Karte wieder vorgelegt und entsprechender Getränkekonsum über die Karte bezahlt.

2.2.1 Bonus

Der Bonus wird als ein Byte gespeichert, daraus ergibt sich der maximale Bonus zu 127, da sonst ein Überlauf auftreten kann. Bonuspunkte werden durch das konsumieren erhöht. Die OffCard-Anwendung kümmert sich um die Verwaltung der Bonuspunkte.

INS_GET_BONUS (0x30) Liefert die aktuell gespeicherten Bonuspunkte.

INS_ADD_BONUS (0x31) Fügt Bonuspunkte hinzu.

Folgende Fehler können geworfen werden:

- **ERROR_ADD_BONUS_OVERFLOW (0xE030)**
 - Es kann kein Bonus mehr hinzugefügt, da sonst ein Überlauf auftreten würde.

INS_SUB_BONUS (0x32) Verbraucht Bonuspunkte.

Folgende Fehler können geworfen werden:

- **ERROR_SUB_BONUS_UNDERFLOW (0xE031)**
 - Subtrahieren von Bonus würde ein Unterlauf-Fehler verursachen.
- **ERROR_SUB_INSUFFICIENT_BONUS (0xE032)**
 - Nicht genug Bonuspunkte auf der Karte.

INS_RESET_BONUS (0x33) Setzt die Bonuspunkte auf der Karte auf Null (Werkszustand).

2.2.2 Geld

Auf dem Disco-Applet können Geldfunktionen aus dem Student-Applet genutzt werden. Dies ist nötig damit Student und Disco nicht über getrennte Guthaben verfügen müssen. Kommunikation und der Zugriff auf das Geld des Student-Applet erfolgt über die Applet-Firewall. Die Anweisungen sind identisch zu den Anweisungen auf dem Student-Applet. Für Details zu den Anweisungen wird auf [Unterabschnitt 2.1.1](#) verwiesen.

2.2.3 Getränke

Auf der SmartCard können maximal 50 Getränke gespeichert werden, welche in der Disco konsumiert wurden. Für ein Getränk wird nur die ID als Byte in einer Liste gespeichert. Der Preis zu dem Getränk wird durch die OffCard-Anwendung der ID zugeordnet.

INS_GET_DRINKS (0x34) Liefert eine Liste von konsumierten Getränken.

INS_ADD_DRINK (0x35) Fügt ein Getränk der Liste hinzu.

Folgender Fehler kann geworfen werden:

- **ERROR_ADD_DRINK_HAD_TO_MUCH (0xE033)**
 - Getränkeliste ist voll, es können keine weiteren Getränke hinzugefügt werden.

INS_SET_PAID_DRINKS (0x36) Anhand einer übergebenen Liste, welche Einsen oder Nullen enthält, wird die interne Getränkeliste bereinigt, um Getränke welche bezahlt wurden. Eine Eins entspricht dabei bereits bezahlt und eine Null noch zu bezahlen. Die Übergebene Liste muss die gleiche Länge haben wie die derzeit gespeicherte Liste auf der Karte.

2.3 Crypto-Applet

Die AID des Crypto-Applets ist Crypto in hexadezimal geschrieben:

- 0x 43 72 79 70 74 6f

Das Klassenbyte für das Crypto-Applet ist:

- 0x 10

Das Crypto-Applet wurde geschaffen um Funktionen zu Verschlüsselung und Signierung für alle Applets über die Applet-Firewall zu bieten. Im Crypto-Applet wird das asymmetrisches kryptographische Verfahren RSA mit einer Schlüssellänge von 512 Bit realisiert. Dieses Applet besitzt im Wesentlichen Funktionen zur Verschlüsselung und Signierung sowie zur Entschlüsselung und Verifizierung.

2.3.1 Funktionsweise

Das Crypto-Applet besitzt folgende Anweisungen:

INS_IMPORT_CARD_PRIVATE_MOD (0x10) Importiert privaten Modulus des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- ERROR_IMPORT_CARD_PRIVATE_MOD (0xE010)
 - Privater Modulus der Karte ist bereits auf der Karte gesetzt.

INS_IMPORT_CARD_PRIVATE_EXP (0x11) Importiert privaten Exponenten des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- ERROR_IMPORT_CARD_PRIVATE_EXP (0xE011)
 - Privater Exponent der Karte ist bereits auf der Karte gesetzt.

INS_IMPORT_CARD_PUBLIC_MOD (0x12) Importiert öffentlichen Modulus des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- **ERROR_IMPORT_CARD_PUBLIC_MOD (0xE012)**
 - Öffentlicher Modulus der Karte ist bereits auf der Karte gesetzt.

INS_IMPORT_CARD_PUBLIC_EXP (0x13) Importiert öffentlichen Exponenten des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- **ERROR_IMPORT_CARD_PUBLIC_EXP (0xE013)**
 - Öffentlicher Exponent der Karte ist bereits auf der Karte gesetzt.

INS_EXPORT_CARD_PUBLIC_MOD (0x14) Exportiert öffentlichen Modulus des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- **ERROR_EXPORT_CARD_PUBLIC_MOD (0xE014)**
 - Exportieren des öffentlichen Modulus des Schlüssel der Karte fehlgeschlagen.

INS_EXPORT_CARD_PUBLIC_EXP (0x15) Exportiert öffentlichen Exponenten des Schlüssel der Karte.

Folgender Fehler kann geworfen werden:

- **ERROR_EXPORT_CARD_PUBLIC_EXP (0xE015)**
 - Exportieren des öffentlichen Exponenten des Schlüssel der Karte fehlgeschlagen.

INS_IMPORT_TERMINAL_PUBLIC_MOD (0x16) Importiert öffentlichen Modulus des Schlüssels der OffCard-Anwendung.

Folgender Fehler kann geworfen werden:

- **ERROR_IMPORT_TERMINAL_PUBLIC_MOD (0xE016)**
 - Öffentlicher Modulus der OffCard-Anwendung ist bereits auf der Karte gesetzt.

INS_IMPORT_TERMINAL_PUBLIC_EXP (0x17) Importiert öffentlichen Exponenten des Schlüssels der OffCard-Anwendung.

Folgender Fehler kann geworfen werden:

- **ERROR_IMPORT_TERMINAL_PUBLIC_EXP (0xE017)**
 - Öffentlicher Exponenten der OffCard-Anwendung ist bereits auf der Karte gesetzt.

Über die Instruktionen werden öffentliche und private Schlüssel auf die Karte importiert. Die OffCard-Anwendung besitzt ein öffentliches und privates Schlüsselpaar. Ebenfalls besitzt die SmartCard so ein Schlüsselpaar. Wird das Applet installiert so sind keine Schlüssel gesetzt, so dass keine Verschlüsselung und Entschlüsselung möglich ist. Zur Verwendung der Karte müssen zunächst die Schlüssel über die OffCard-Anwendung generiert und dann auf die Karte importiert werden. Es ist nicht möglich die Schlüssel im Nachhinein zu Ändern (um Manipulation der Karte zu verhindern).

Für die MultiCard sowie dazugehörige OffCard-Anwendung existiert nur ein Schlüsselpaar für die OffCard-Anwendung und ein Schlüsselpaar für die OnCard. Sollte ein Dritter im Besitz einer SmartCard im Werkzustand bekommen und selbst die Schlüssel generieren, so ist das System dennoch komplett sicher. Dem Angreifer ist es nicht möglich die Daten von der OffCard-Anwendung zu entschlüsseln, da der selbst generierte Schlüssel der Karte die empfangenen Daten nicht entschlüsseln kann. Anders herum kann von der OnCard-Anwendung an die OffCard-Anwendung gesendete Daten nicht entschlüsselt werden. Begründet ist dies damit, dass die

Schlüssel von OnCard und OffCard nicht zueinander passen. Im Wesentlichen ist die manipulierte SmartCard unbrauchbar. Sollte ein Dritter im besitzt der Schlüssel für OffCard und SmartCard sein, so ist ist das System unsicher.

Die Applets Student und Disco besitzen die Möglichkeit über die Applet-Firewall eine Instanz des Crypto-Applets zu erhalten und somit die Funktionen zur Ent- und Verschlüsselung zu verwenden.

2.3.2 Verschlüsselung

Bei der Verschlüsselung werden die der Funktion übergebenen Daten mit Hilfe des privaten Schlüssel der Karte signiert. Außerdem erfolgt eine Verschlüsselung der Daten mit dem öffentlichen Schlüssel der OffCard-Anwendung. Die Daten werden im Anschluss in den Puffer gespeichert, sodass das Applet, welches die Verschlüsselungs-Funktion aufgerufen hat, diese Daten versenden kann. Bei ein- und ausgehenden verschlüsselten Daten hat der Puffer folgenden Aufbau:

Klassenbyte | Instructionbyte | Parameter 1 | Parameter 2 |

Länge der Daten: 128 | 64 Byte Daten + 64 Byte Signatur |

Länge zu sendender Bytes

2.3.3 Entschlüsselung

Die Entschlüsselungs-Funktion entschlüsselt mit Hilfe des privaten Schlüssel der Karte 64 Bit Daten. Der durch die Entschlüsselung generierte Klartext wird durch den öffentlichen Schlüssel der OffCard-Anwendung sowie der mit übertragenen Signatur verifiziert. Dies Verhindert eine Manipulation von Daten durch einen Dritten. Sollten die Daten manipuliert worden sein, wird der Fehler:

- ISO7816.SW_DATA_INVALID

geworfen. Im Anschluss wird der Klartext zur weiteren Verwendung in den Puffer gespeichert, falls die Daten korrekt verifiziert wurden.

3 OffCard

3.1 Simulation

Für die Benutzung der OffCard-Anwendung mit der simulierten SmartCard muss in der `opencard.properties` Datei die Konfiguration für die Simulation aktiv sein. Die Konfiguration für die reale SmartCard muss mit Zeilenkommentaren (`#`) deaktiviert werden. Die Simulation der SmartCard muss im Eclipse gestartet werden. Anschließend muss das Terminal mit dem Port 8050 geöffnet werden. Dazu kann folgender Befehl verwendet werden: `/terminal "Remote|localhost:8050"` Nach dem Freigeben der Verbindung mit `/close` kann die OffCard-Anwendung gestartet und benutzt werden.

3.2 Connection-Tab

todo

3.3 Configuration-Tab

todo

3.4 Student-Tab

todo

3.5 Disco-Tab

4 Fazit

todo