InterCard AG

Verwendung des Mifare DESFire-Chip EV1 8 KByte durch InterCard

Mifare DESFire EV1

Der Mifare DESFire EV1 Chip ist eine Entwicklung von NXP, Eindhoven (Holland). Es handelt sich um einen Prozessorchip in kontaktloser Ausführung. Die Verbindung zwischen Chipkarte und Chipkartenleser wird per Funk aufgebaut. Daher fällt dieser Chiptyp unter die Gattung der RFID-Systeme. Die Stromversorgung wird vom Chipkartenleser übernommen. Sobald der Chip in das Feld eines Chipkartenlesers kommt, erhält der Chip von dem Leser ausreichend Strom zur Verarbeitung.

Die Komponenten eines Prozessorchips sind vergleichbar mit einigen Komponenten eines Computers. Der Chip besitzt einen nicht flüchtigen Speicher, einen Prozessor, einen kryptographischen Co-Prozessor, einen Arbeitspeicher, ein Interface sowie ein Betriebssystem mit eigenem Befehlssatz. Wie bei einem Computer wird nach dem Vorhalten der Karte vor ein Lesegerät das Betriebssystem gestartet. Es werden Dateien geöffnet und verarbeitet.

Die Größe des Speichers innerhalb des Prozessorchips beträgt 8kByte. Dieser Speicher wird belegt mit den Nutzdaten für den Anwender, mit den Zugriffsschlüsseln für die Dateien und den Verwaltungsdaten der Karte.

Alle Daten können mit unterschiedlichen und allgemein bekannten Algorithmen verschlüsselt werden. Es stehen die Algorithmen DES, 3DES und AES zur Verfügung, wobei von InterCard nur der AES-Algorithmus angewendet wird.

Im Speicher des Mifare DESFire EV1 Chip finden insgesamt bis zu 28 Applikationen Platz. Jede Applikation kann mit bis zu 32 Dateien angelegt werden. Jede Datei verfügt über einen eigenen AID (Application IDentifier) und ist somit eindeutig erkennbar. Im Gegensatz zu dem Mifare-Classic-Chip, bei der die AID im sogenannten Mifare Application Directory (MAD) hinterlegt werden, besitzt die Mifare DESFire EV1 ein selbstverwaltetes Inhaltsverzeichnis. Somit können von den Karten die aktivierten Applikationen (AIDs) abgefragt werden.

Es werden insgesamt 5 unterschiedliche Dateitypen unterstützt. Abhängig von dem verwendeten Dateityp kann über einen integrierten Backup-Mechanismus sichergestellt werden, dass beim Schreiben von Daten auf die Karte Inkonsistenzen verhindert werden, wenn z.B. die Karte zu früh aus dem Empfangsfeld des Lesers entfernt wird.

Die Schlüssel im Chipkartenleser zum Lesen und Schreiben von Dateien auf dem Chip werden auf einem Sicherheitsmodul – dem sogenannten SAM – vorgehalten. Dieses Modul besteht ebenfalls aus einem Prozessorchip und ist vergleichbar mit der „SIM-Karte“ in einem Handy.

Die Zugriffsberechtigungen für die einzelnen Dateien werden über eigene Schlüssel definiert, jeweils nach dem Anwendungsszenario auch unterschiedlich für Lesen, Schreiben und Konfiguration. Dabei wird auch der nachträgliche Tausch von Schlüsseln auf bereits ausgegebene Karten, z.B. im Falle einer Schlüsselkompromittierung, unterstützt.

InterCard belegt den Mifare DESFire EV1 Chip mit insgesamt 6 Applikationen:

- Allgemeine Daten
- Hauptbörse
- Kontingentbörse
- Subventionsbörse
- Persönliche Daten
- Zugang und Zeiterfassung

Innerhalb dieser Applikationen werden Daten zum Karteninhaber wie zum Beispiel

- Matrikelnummer oder Personalnummer
- Bibliotheksbenutzernummer
- Zugangsnummer
- Zeiterfassungsnummer
- Merkmale für Kassensysteme
- Gültigkeitsdatum

hinterlegt.

Es stehen dem Nutzer diverse Börsen für viele Zahlungsmöglichkeiten innerhalb einer Institution oder einem Verbund zur Verfügung.

Für Zugangssysteme ohne Vernetzung, den sogenannten Offline-Systemen, sind entsprechende Dateien in den Applikationen vorgesehen.

Durch die jahrzehntelange Erfahrung im multifunktionalen Umfeld sind mit Auslieferung der Karte bereits alle Vorkehrungen getroffen, um die Chipkarte flexibel in allen Bereichen nutzen zu können. Außerdem steht noch ausreichend Speicherbereich für eigene Lösungen zur Verfügung. Somit können nachträglich beliebige Applikationen und auch Dateien in bestehende Applikationen auf die Karte aufgebracht werden. Der durchdachte Aufbau der Chipkarte macht dies möglich.

Technische Details

Name	Mifare DESFire EV1
Normung	Nach ISO/IEC 14443 Type A und ISO/IEC 7816
Datenübertragung	13,56 MHz
Transaktionszeiten	< 1000 ms
Reichweite	bis zu 100 mm (abhängig von Antennen-geometrie und Gehäuseform des Lesegerätes)
Speicherkapazität	8 kByte
Aufteilung des Speichers	Max. 28 Applikationen mit jeweils bis zu 32 Dateien
Seriennummer	7 byte, eindeutig und unveränderlich
Verschlüsselungsalgorithmen	DES und 3DES mit 56, 112, 168 bit Schlüssellänge AES mit 128 bit Schlüssellänge