Java basierende Chipkartenanwendungen

Horst H. Henn

IBM Deutschland Entwicklung GmbH, Böblingen

ChipCard 97 - Die Chipkarte in Wirtschaft und Verwaltung

29. und 30. September 1997 in Seeheim-Jugenheim

Abstract: Networked Java applications can provide consistent service for multifunction smartcards. Java application functions can be distributed on cards, clients and servers according to application needs. The role of PC/SC, OpenCard and JavaCard to provide the necessary common functions and infrastructure for smartcard applications is described.

Chipkarten im Netzwerk

Netzwerkdienste ergänzen oder ersetzen zunehmend bestehende Geschäftsverfahren oder stellen neuartige Dienstleistungen zur Verfügung. Verbesserung der Kundenbeziehungen, Öffnung der internen Geschäftsabläufe für Geschäftspartner oder Kunden sowie Standardisierung und Globalisierung interner Verfahren werden durch Nutzung der Internet Technologie ermöglicht. Neben dem Personal Computer als Benutzerschnittstelle werden zunehmend auch andere Endgeräte wie zum Beispiel Netzwerk Computer(NC), Telefone, Kioske, Kleincomputer (Organizer) Kassensysteme, Fernsehgeräte u. a. im Internet unterstützt. Dadurch werden zusätzliche Dienste ermöglicht und bestehende Dienste können in einer erweiterten Infrastruktur angeboten werden. Typisch ist zum Beispiel die Erweiterung des Personal Computers als Endgerät für Telefondienste, Rundfunk und Fernsehen oder die Erweiterung der öffentlichen Telefone zum Serviceterminal für Banken, Kreditkartenorganisationen und Verkehrsbetriebe. Identifizierung des Kunden durch eine PC Hardwareadresse oder eine physikalische Netzwerkadresse ist in solchen Systemen nicht mehr praktikabel.

Diese erweiterte Infrastruktur ermöglicht optimierte, integrierte Dienstleistungen für den Kunden stellt aber auch neue Anfoderungen an Organisation und Technologie. Akzeptanz dieser neuen Dienste bei Kunden erfordert attraktive Angebote, einfach zu benutzende und konsistente Benutzerschnittstellen, Schutz vor Mißbrauch speziell persönlicher Daten sowie Zuverlässigkeit und hohe Verfügbarkeit der Dienste. Für die Dienstanbieter sind die eindeutige Identifikation des Kunden als Grundlage für Zugriff, Abrechnung und Datensicherheit sowie die Infrastruktur zur Verteilung von Programmen und Daten von besonderer Bedeutung. Proprietäre Netzwerke werden zunehmend durch generelle Netzwerkdienste abgelöst, die von vielen Anbietern mit geringen Kosten benutzt werden können. Voraussetzung ist hierfür aber die weitgehende Standardisierung sowohl der Funktion als auch der Verwaltung der Teilnehmer, Applikationen und Daten.

Chipkarten können in dieser offenen Systemumgebung wesentliche Funktionen übernehmen:

- Konsistente Benutzerschnittstellen und einfache Benutzung durch Speichern von Identifikation, Profilen, Serviceadressen (URLs), Referenzen, usw
- Kombination von Anwendungen auf einer Chipkarte z.B. Bankkarte/Kreditkarte/Reisen oder Identifikation/Führerschein/ Versicherung u.a.
- Identifikation des Kunden durch Authentizierung, PIN oder Passwort, Zertifikate und Digitale Signatur
- Sichere Speicherung von Kundennummern, Schlüsseln und Zertifikaten (Secure Token)
- Unterstützung sicherer Kommunikationsprotokolle im Netzwerk

Moderne Chipkarten Operating Systeme erlauben es mehrere Applikationen auf einer Karte statisch, zum Beispiel bei der Herausgabe, oder dynamisch inklusive der notwendigen Schlüssel oder Zertifikate während des Betriebs zu laden. Hierfür werden weitgehend proprietäre Funktionen für das Systemmanagement eingesetzt, da dieser für den Betrieb eines Systems wichtige Aspekt bisher durch bestehende Standards nicht abgedeckt wird. Der Standard ISO/IEC 7816-5 [1] bietet hingegen ein Regelwerk für die Vergabe von Applikations Identifikationsnummern, das als Basis von Chipkartenanwendungen im Netzwerk geeignet ist. Auf der Basis dieses Standards können Daten für spezifische Anwendungen zum Beispiel von Industrieverbänden oder anderen Organisationen definiert und eindeutig klassifiziert werden. Häufig werden jedoch zusätzliche Funktionen, die spezifisch für die jeweilige Applikation sind, benötigt. Diese werden bei typischen auf dem ISO/IEC 7816 Standard basierenden Karten vom Kartenherausgeber zur Verfügung gestellt und sind abhängig vom jeweiligen Kartenbetriebssystem und der Kombination der Anwendungen auf der Karte.

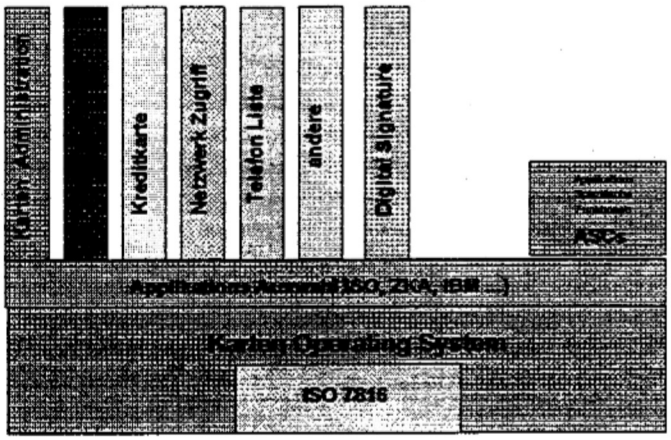

Abbildung 1: Multifunktionale Chipkarte - Selektion der Applikation

Java - Basis für Chipkartenanwendungen

Für jede Chipkartenbasis und für jede Anwendung muß im Netzwerk ein komplementäres Applikationsprogramm inklusive der Schlüssel und Sicherheitsdienste bereitgestellt werden. Die Verteilung der Anwendungen durch Hardwaremodule und der Schlüssel mittels Sicherheitsmodulen (SAM - Security Access Module), wie zum Beispiel bei Kreditkartenanwendungen üblich, ist bei Anwendungen im Netzwerk nicht handhabbar. Die Endgeräte müßten eine Vielzahl von Sicherheitsmodulen vorhalten; deren Kontrolle und Verwaltung in ungesicherter Umgebung ist zu unzuverlässig. Die Kunden sind in der Regel nicht bereit, mehrere Sicherheitssysteme zu installieren und zu benutzen. Die Applikationsprogramme und Schlüssel müssen mit standardisierten Verfahren verteilt und gespeichert werden.

Die Vielzahl der verschiedenen Endgeräte mit unterschiedlichen Betriebssystemen erfordert Anpassungen der Applikationsprogramme und Softwareverteilung, Systemmanagement und -test werden extrem komplex und aufwendig. Zusätzlich müssen diese Systeme im laufenden Betrieb auf neue Technologien bei Chipkarten und Geräten angepaßt werden.

Java in Kombination mit Internet bietet Lösungselemente für die Implementierung multifunktionaler Kartensysteme.

- Zugriff auf beliebige Anwendungen im Netz ist möglich
- Applikationsprogramme können als Java Applets zentral erstellt und verwaltet werden
- Java Applets sind auf einer Vielzahl von Plattformen lauffähig. Eine spezielle Version von Java ist sogar auf Chipkarten lauffähig (JavaCard).
- Sicherheitsdienste können im Netzwerk zur Verfügung gestellt werden. Standardisierte Sicherheitsfunktionen von Java für die Verteilung und Ablaufsteuerung von Programmen können genutzt werden.
- Java Applikationen sind im Kontext von Browsern lauffähig. Dadurch können dem Benutzer vertraute Funktionen für Suchen, Selektion, Adressierung und Verwaltung eingesetzt werden.

- Die Chipkarte kann als Plattform unabhängiger Träger von Zugriffsdaten, Schlüsseln und Applikationen dienen.

Ein wesentliches Prinzip von Java ist die Beschränkung des Zugriffs von Applikationsprogrammen auf lokale Resourcen in den Geräten. Der Zugriff auf Chipkartenlesegeräte und Chipkarten ist mit Standardverfahren nicht möglich. Hierfür muß in Java eine standardisierte Schnittstelle zu Chipkartenlesegeräten und Chipkarten eingeführt und von den Herstellern von Java Systemen als Applikations Programm Schnittstelle (API) unterstützt werden. Da Java Systeme in der Regel nicht direkt auf Hardware lauffähig sind, sondern auf Plattformen wie WINDOWS, UNIX, OS/2 u.a.aufsetzen, müssen die Hardware der Chipkartentergeräte und APIs für diese Geräte und Karten definiert werden. Obwohl sich verschiedene Gremien mit der Standardisierung von Geräteschnittstellen befaßt haben (u.a. EMV, in Deutschland MKT im Gesundheitswesen) gibt es zur Zeit keine von vielen industriellen Herstellern unterstützten Standards wie zum Beispiel bei Druckern oder Diskettenlaufwerken. Deshalb haben sich verschiedene Industriekonsortien gebildet, um diese Standards zu definieren und auch Geräte und Software, die diesen Standards genügen, am Markt verfügbar zu machen.

Das PC/SC Konsortium [2] hat es sich zur Aufgabe gemacht sowohl die Hardware der Chipkartenterminals als auch die Applikationsprogramm Schnittstellen für die Windows 95 und Windows NT Plattform zu definieren. Chipkartenterminals z.B. in PCs oder Tastaturen fest eingebaut, über serielle Schnittstellen (RS-232C, USB) oder über PCMCIA/JEIDA angeschlossen, werden über einheitliche Schnittstellen angesprochen.

Das OpenCard Forum [3] definiert Chipkarten APIs für Java speziell für Network Computer aber auch für andere Plattformen.

Das JavaCard Forum [4] definiert eine Java Schnittstelle für Java Applikationen, die auf Chipkarten ausgeführt werden können.

PC/SC

Das PC/SC Konsortium hat es sich zum Ziel gesetzt, Interoperabilität von Chipkartengeräten und Chipkarten durch Vereinbarungen der führenden Anbieter zu erreichen. Aus der Vielzahl der vorhandenen Standards werden hierfür geeignete Elemente ausgewählt und durch Definition von Applikationsschnittstellen ergänzt, sodaß die Anwender vollständig definiertes Systen nutzen können. PC/SC Spezifikation definiert folgende wesentliche Elemente:

- Integrated Circuit Card (ICC) - Chipkarte
  Genereller Begriff für alle Typen von Chipkarten, speziell Prozessorkarten mit T=0 und T=1 Kommunikations Protokoll, spätere Erweiterung auf Speicherkarten gemäß ISO7816-10. Obwohl in der PC/SC Spezifikation auch ein spezielles Kartenbetriebssystem definiert wird, können generell alle Karten, die der PC/SC Hardware Spezifikation genügen, unterstützt werden.
- Interface Device (IFD) - Chipkarten Lesegerät
  Diverse Typen von Chipkartenterminals
- Interface Device Handler (IFD Handler) - Geräte Treiber
  wird in der Regel vom Hersteller des Lesegeräts erstellt und als Bestandteil des Betriebssystems installiert
- ICC Resource Manager
  Funktion des Betriebssystems zum Anschluss von Lesegeräten und zur Verwaltung von Geräten und Chipkarten (ähnlich Print Manager)
- ICC Service Provider
  Ein Basisapplikationsprogramm, das für einen Typ von Chipkarte bestimmte Schnittstellen für Applikationen zur Verfügung stellt.
- Crypto Service Provider
  Ein Applikationsprogramm, das über Schnittstellen und Funktionen für Crypto Dienste verfügt
- ICC Aware Application
  Ein Applikationsprogramm, das eine Chipkarten Anwendung implementiert und in der Regel mit dem ICC Resource Manager, dem ICC Service Provider und dem Crypto Service Provider kommuniziert.

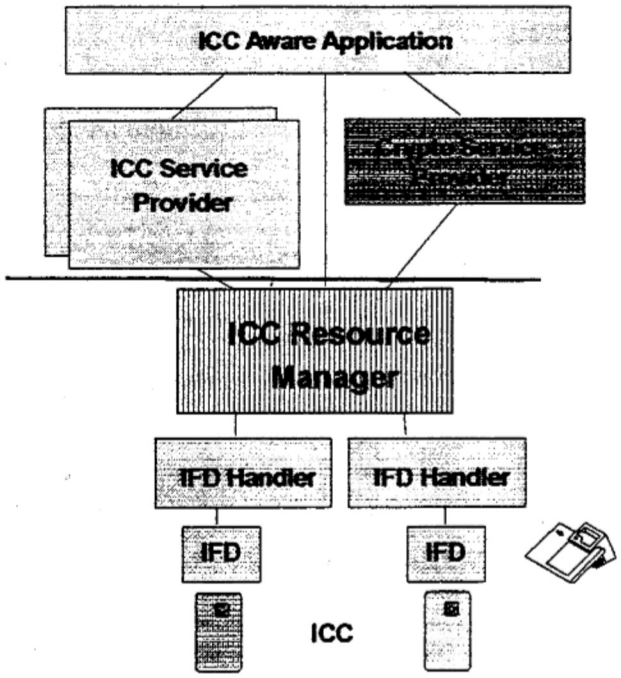

Abbildung 2: PC/SC Struktur

Die PC/SC Spezifikation wird für WINDOWS 95 und WINDOWS NT implementiert, PC/SC kompatible Geräte werden von mehreren Herstellern bereits angeboten. Für den Anwender steht damit ein komplettes System von Geräten, Betriebssystemdiensten and APIs für Chipkartenanwendungen auf den Plattformen WINDOWS 95 und und WINDOWS NT zur Verfügung. Der ICC Resource Manager erlaubt es, Lesegeräte ähnlich wie Drucker zu verwalten und von verschiedenen Anwendungen zu nutzen. Der ICC Resource Manager erlaubt es auch Chipkarten zu verwalten und eine logische Verbindung zu dem zugehörigen Applikationsprogramm (ICC Service Provider) unter Kontrolle des Betreibssystems herzustellen.

Da PC/SC 32 Bit Schnittstellen und spezielle Funktionen des Plattformbetriebssystems benutzt, kann diese Schnittstelle auf einfacheren Plattformen wie z.B. Windows 3xx oder DOS nicht implementiert werden. Auch auf anderen Plattformen wie z.B. UNIX, OS/2 oder Kontroll Programmen für Gerate (Embedded System) steht die PC/SC Funktionalität nicht zur Verfügung. Vom PC/SC Konsortium wird deshalb auf diesen Plattformen die Implementierung einer PC/SC Migrationsschnittstelle empfohlen, die eine Teilfunktion von PC/SC definiert und eine einfache Portierung von Applikationen auf die PC/SC Plattform erlaubt. Der Funktionsumfang dieser Schnittstelle ist stark eingeschränkt z.B. können Lesegeräte nur von einer Applikation aus genutzt werden. Dies ist jedoch häufig für einfache Geräte und für PCs mit dedizierten Applikationen ausreichend.

OpenCard

Das OpenCard Konsortium definiert ähnlich wie PC/SC eine Applikationsschnittstelle für Chipkartenanwendungen, diese wird jedoch an die speziellen Anforderungen der Java Umgebung angepaßt. Durch Harmonisierung der Arbeiten im PC/SC Konsortium und dem OpenCard Konsortium soll erreicht werden, daß die Schnittstelle zu den Applikationen vergleichbare Funktionen und Schnittstellen aufweist. OpenCard definiert keine Hardware Schnittstellen sondern verweist auf die PC/SC Hardware Definitionen. OpenCard implementiert die Funktionen zur Verwaltung der Geräte und Karten in Java . In Windows 95 und Windows NT Umgebung werden die Funktionen von PC/SC hierfür genutzt. Mehrere Java Anwendungen können ein installiertes Chipkartengerät nutzen, das zum Beispiel über eine PC/SC Migration Schnittstelle angeschlossen ist. Dadurch kann OpenCard auch auf anderen Plattformen als PC/SC genutzt werden.

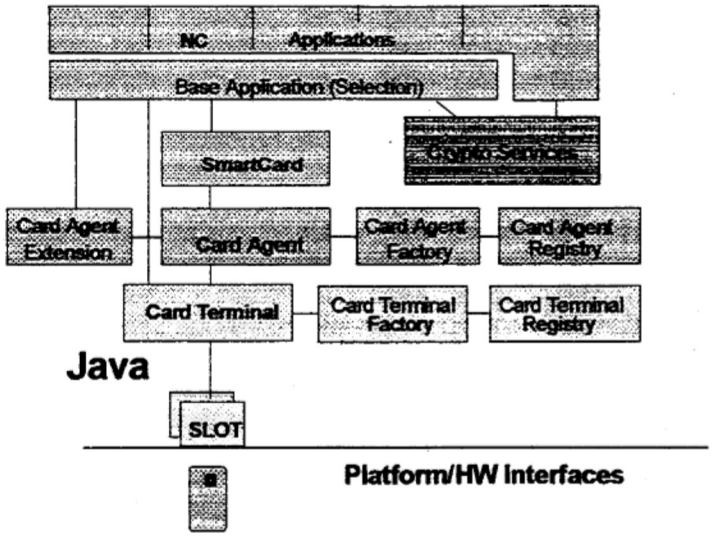

Abbildung 2: OpenCard Struktur

Während OpenCard ähnliche Funktionen wie PC/SC zur Verwaltung der Lesegeräte und Karten bereitstellt, strukturiert OpenCard die Applikationsunterstützung (PC/SC - Service Provider) durch

- Card Agent - eine Funktion, die Anwendung vom Chipkartenbetriebssystem und Sicherheitsfunktionen weitgehend entkoppelt.
- Unterstützung multifunktionaler Chipkarten durch Applikationsselektion und -verwaltung

Auf Windows 95 oder Windows NT Plattformen übernimmt OpenCard die Funktion eines speziellen Service Providers, der Java Schnittstellen und das Java Netzwerkmodell unterstützt.

JavaCard

Das JavaCard Forum definiert eine Applikationsschnittstelle für Java Anwendungen, die auf einer Chipkarte lauffähig sind. Hierfür werden eine vereinfachte Java Virtuelle Maschine, Klassen für Chipkarten spezifische Funktionen sowie Schnittstellen für die Entwicklung von Anwendungen und den Betrieb der Karte spezifiziert. JavaCard definiert also im Gegensatz zu ISO 7816 kein Kartenbetriebssystem sondern nur die Schnittstelle zu den Applikationen. Die Implementierung dieser Schnittstellen in spezifischen Betriebssystemen bleibt den Herstellern überlassen ähnlich wie die Implementierung von Java Systemen.

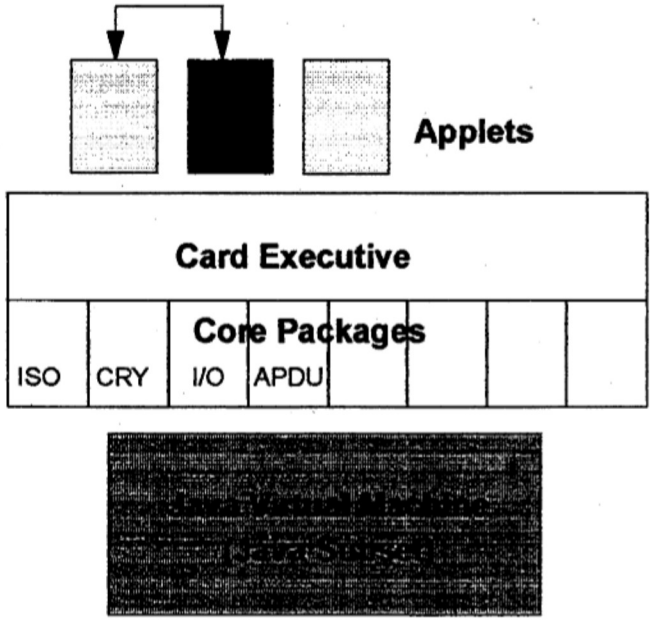

Abbildung 3: JavaCard Struktur

Ziel der JavaCard Initiative ist es, Anwendern die Erstellung von speziellen Applikationsprogrammen auf Chipkarten mit generell verfügbaren Werkzeugen zu ermöglichen. Bei heute üblichen Chipkartensystemen müssen Anwednungen mit dem Kartenbetriebssystem integriert werden, da keine Schnittstellen für Anwendungen und auch keine Trennung von Betreibssystem und Anwendung architekturiert und implementiert sind.

JavaCard verwendet für die Kommunikation mit Geräten und Anwendungsprogarmmen die in ISO/IEC 7816 definierten Protokolle. Karten, die der JavaCard Spezifikation entsprechen, können damit im PC/SC und OpenCard Umfeld betrieben werden.

JavaCard erlaubt eine weitgehende Entkopplung von Herstellung und Herausgabe von Chipkarten von den Applikationen, die auf der Chipkarte verfügbar sind. Dadurch können technische, organisatorische und strukturelle Abhängigkeiten für Chipkartensysteme minimiert werden.

Typische Anwendungen

Typische Java basierende Chipkartenanwendungen nutzen die Internet Struktur um Applikationen für Geschäftspartner oder Kunden bereitzustellen, ohne daß spezielle Software bei den Partnern installiert werden muß. Voraussetzung ist allerdings, daß zum Beispiel OpenCard als generelle Schnittstelle für Java Anwendungen verfügbar ist.

Der Kunde greift zum Beispiel mit Hilfe eines Browers auf die Heimseite des Anbieters zu auf der eine spezielle Anwendung für Chipkarten selektiert werden kann. Durch die Selektion wird ein spezielles Applet in das Gerät oder den PC des Kunden geladen und die für diesen Geschäftsvorgang relevante Chipkartenapplikation selektiert. Beliebige Anwendungen, Sicherheitsprüfungen usw können dann durchgeführt werden, Benutzerprofile können zur Optimierung der Ablaufsteuerung verwendet werden. Auf der Karte gespeicherte Schlüssel oder Zertifikate können zum Beispiel für Secure Socker Layer Services genutzt werden.

Durch Kombination von Chipkarte, Browser und HTML Dokumenten lassen sich eine Vielzahl von Anwendungen ohne aufwendige individuelle Programmierung implementieren z.B.

- Kundeninformatinssysteme
- Bestell- und Auftragssteuerung
- Internet Vorzugsdienste
- Angebotserstellung
- Zahlungssysteme

Systemmanagement und Betrieb

Die Infrastruktur für Chipkartenanwendungen wird durch Einführung der PC/SC, OpenCard und JavaCard Industriestandards wesentlich verbessert und gegliedert. Ersmals stehen für den Anwender integrierte Systeme anstatt inkompatibler Einzelkomponenten zur Verfügung. Eine wesentliche Komponenten für Chipkartensysteme ist jedoch noch nicht oder nicht eindeutig definiert oder nicht allgemein unterstützt. Es fehlt ein gemeinsamer Standard für die Speicherung und Verteilung von Schlüsseln und Zertifikaten und die entsprechenden APIs auf mehreren Plattformen. Individuelle Lösungen auf proprietären Plattformen mit ähnlicher Funktionalität stehen aber zur Verfügung, sodaß ein gemeinsamer Standard relativ schnell definiert werden könnte. Dieses Problem kann jedoch auch durch die Verteilung von Schlüsseln mittels der Chipkarte umgangen werden.

Für die Initialisierung, Personalisierung und das Systemmanagement von Chipkarten sind zur Zeit nur proprietäre Lösungen verfügbar. Es zeichnet sich zur Zeit auch kein Standard ab, da dies einen Konsens der Hersteller und der Betreibergesellschaften erfordern würde, der allenfalls im Rahmen von großen internationalen Projekten erzielt werden kann. Für die Anwendung und die Funktion von Chipkartensystemen hat die mangelnde Standardisierung in diesem Bereich jedoch geringen Einfluß.