



**Geheim:**  
In diesem  
Beispiel sind  
verschlüs-  
selte Zellen  
und davon  
abhängige  
nur noch mit  
Chipkarte  
lesbar

# Smartcards nach Maß

*Auf Telefon- und künftigen EC-Karten bringen die Chips millionenfach Nutzen. Jetzt sind Zeit und Technik reif, sie nach eigenem Geschmack für Kleinserien anzufertigen.*

Chipkarten sind bisher vor allem Big Business: Mit Telefonkarten ist praktisch die gesamte Bevölkerung ausgestattet, und wenn die Banken ihren Kunden demnächst EC-Karten mit Geldbörsenfunktion andienen, sollen die Prozessorkärtchen in einer Auflage von 50 Millionen über den Banktresen gehen.

Das metallisch schimmernde Plättchen auf dem Plastik ist dem Anwender jedoch ein Buch mit sieben Siegeln: Je nach seiner Programmierung erweckt es Telefonautomaten oder Geldausgabegeräte zum Leben. Daß eine derartige Smartcard gleichermaßen der Schlüssel zum PC, Kopierer, Getränkeautomaten oder zur Firmentür sein könnte oder die Ver- sowie Entschlüsselung und das Signieren elektronischer Dokumente ermöglicht, erscheint dagegen wie ein bizarrer Traum.

## Ein einfaches „Sesam, öffne dich“ genügt nicht mehr

Doch tatsächlich können Software-Entwickler die High-Tech-Karten mit relativ bescheidenem Aufwand in den Dienst

der eigenen Sache stellen: Die israelische Firma Aladdin Knowledge Systems bietet das *Aladdin Smartcard Environment* (ASE) an, mit dem Chipkarten in eigene Anwendungen eingebunden werden können. Typische Beispiele sind neben der elektronischen Geldbörse Zugangskontrolle oder Verschlüsselung – Anwendungen also, bei denen es darum geht, daß bestimmte Leistungen oder Informationen nur Berechtigte bekommen dürfen. Und da hat die Chipkarte ihre Vorteile gegenüber den reinen Software-Lösungen:

- Wo sonst nach einem Kennwort gefragt wird, muß zusätzlich das Kärtchen gezückt werden.
- Anstatt Geheimschlüssel auf der Festplatte abzulegen, ruhen sie nicht auslesbar in einer Prozessorkarte.
- Ver- und Entschlüsselung erledigen spezialisierte Kryptokarten, von Experten geschrieben und recht sicher vor neugierigen Blicken.
- Die Kommunikation vom Rechner zur Karte wird bei ASE mit Kryptoverfahren vor Angriffen geschützt.

Große Datenmengen können die Kärtchen aber nicht bewältigen, weil sie zwar

hochspezialisiert, doch keine Superrechner sind. Auch läuft der Datentransfer zum PC nur mit Modemgeschwindigkeit.

## Entwicklung ist jetzt leichter

Wie auch immer Entwickler ihre Software mit Prozessor- oder den als tragbare Datenspeicher funktionierenden Memory-Karten aufwerten wollten – bisher war die größte Hürde, daß sie sich mit den Befehlssätzen der Kärtchen auseinandersetzen mußten. Dies erspart ihnen nun eine Programmierschnittstelle.

Mit Hilfe der zur Kommunikation zwischen Anwendungssoftware und Karte oder Kartenleser nützlichen Bibliothek erledigt man übliche Aufgaben über Funktionsaufrufe aus gängigen Programmiersprachen wie C, C++, Visual Basic und Pascal: das Ein- und Ausschalten der Smartcards etwa oder den Umgang mit deren Dateien und Paßwörtern. Möglich ist dies bislang bei der Entwicklung unter DOS, Windows 3.x, Windows 95 und Windows NT.

So kann dann zwar nicht Hinz und Kunz, jedoch jeder ernsthaft Interessierte in die Chipkarten-Ära starten. Deren Anzahl in der ledernen Geldbörse muß allerdings dadurch nicht drastisch steigen: Eine Chipkarte kann mehrere Funktionen ausführen und bei Bedarf mit unterschiedlichen Paßwörtern absichern.

Karlhorst Klotz



Das ASE-Laufwerk paßt in 3,5-Zoll-Einschübe oder kann extern (serielle oder paralleler Port, 90 cm kurzes Kabel) benutzt werden. Stromversorgung auch mit Batterien möglich. Preis der Entwicklungsumgebung (Laufwerk, Software und Muster-Chipkarten): etwa 580 Mark

Fast Security AG, Gabriele-Münter-Str. 1, 82110 Germering, Tel. (089) 89 42 21 0, Fax 894221-40

<http://www.aks.com>