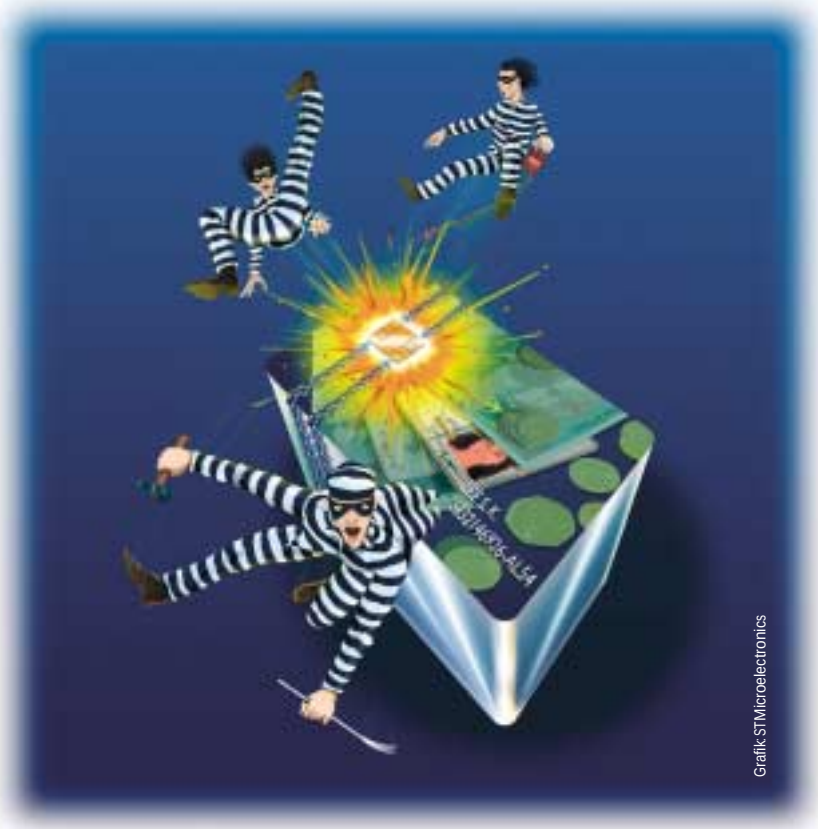
Mehr Sicherheit bei Smartcards



Alfred Vollmer ***Der Abschwung des Handymarktes hat auch bei den Smartcards (Controller-Chipkarten) tiefe Dellen in der Umsatzstatistik hinterlassen: So berichtete Infineon Technologies beispielsweise von einem Umsatzrückgang bei Smartcard-ICs für das letzte Kalender-Quartal 2001 von 47% im Vergleich zum entsprechenden Vorjahresquartal und der weltweit größte Chipkarten-Hersteller Gemplus war sogar noch stärker betroffen, da SIM-Karten für Handys fast 75% seines Geschäfts ausmachen. Dennoch soll der Markt nach Ansicht einer im Herbst 2001 von Frost&Sullivan veröffentlichten Studie von 1,79 Millionen eingesetzten Smartcards im Jahr 2000 auf 3,66 Milliarden Stück im Jahr 2004 anwachsen. Welche Trends sich bei Smartcards abzeichnen und welche Produkte dabei zum Einsatz kommen, um auch die nächsten Chipgenerationen sicher zu machen, erläutert Ihnen der folgende Beitrag.***

Bleiben wir zunächst kurz bei Infineon, die sich genauso wie STMicroelectronics und Philips Semiconductors als Marktführer bei Smartcards sehen. Das deutsche Unternehmen hat vom US-amerikanischen Verteidigungsministerium DoD (Department of Defense) den prestigeträchtigen Auftrag bekommen, die Mikrocontroller-Chips für den CaC (Common Access Card) genannten, neuen Ausweis der rund vier Millionen zivilen, militärischen und externen Mitarbeiter des DoD zu liefern, wobei die fertigen Ausweise von SchlumbergerSema stammen werden.

Der CaC-Chip basiert auf einer offenen Java-Plattform und bietet neben den Sicherheits-Features auch die Möglichkeit, zusätzliche Anwendungen auf die CaC-Karten zu laden.

Im Bereich der kontaktlosen Chipkarten kooperiert Infineon seit kurzem mit Sony bei der Entwicklung kompletter Kontaktlos-Systemlösungen für den Volumenmarkt, die neben multiapplikations-fähigen Chipkarten auch Lesegeräte sowie Hintergrund-Infrastrukturtechnik umfassen. Diese kontaktlosen Chipkarten können unter anderem als elektronische Tickets, Firmen- oder Behördenausweise sowie als Bankenkarten eingesetzt werden. Erste Chips aus der gemeinsamen Entwicklung sollen Ende des Jahres verfügbar sein.

Saftety First

Dass die Sicherheits-Features einer Smartcard an erster Stelle stehen, dürfte sich mittlerweile herum gesprochen haben, denn der Sicherheitsaspekt ist der direkte Grund für den Einsatz von Smartcards. „Die Herausforderung besteht darin, eine offene Smartcard-Plattform an zu bieten, die gleichzeitig auch noch die nötigen Sicherheitsfeatures anbietet unter dem Motto *Open And Safety*", erläuterte Jean-Paul Thomasson, Marketing Director der Smartcard Division bei STMicroelectronics.

Allerdings ist die Chipkarte nur ein Teil innerhalb eines Chipkarten-Systems, der auch den Kartenleser und die Software inklusive Betriebssystem mit einschließt. Aus diesem Grund arbeiten auch diverse Unternehmen im Rahmen von zwei MEDEA+-Projekten an derartigen Konzepten.

Im Projekt A302 EsPass-IS (Enhanced Smartcard Platform for Accessing Securely Services of the Information Society) geht es beispielsweise darum, die Hardware und Software im Rahmen einer offenen Smartcard-Plattform zu schaffen. „Dabei müssen wir beachten, dass die Situation sich derzeit beachtlich verändert", führte Thomasson im Rahmen einer MEDEA+-Präsentation im Dezember 2001 weiter aus. „Der Trend geht hin zur multifunktionalen Karte, auf die Anwendungen herunter geladen werden können – natürlich virenfrei."

Ein weiteres Ziel dieses MEDEA+ - Projekts ist die Entwicklung der entspre-

chenden Sicherheits-Gegenstücke zur Chipkarte auf der Terminal-Seite. „Außerdem müssen wir Test-Strategien und Sicherheits-Roadmaps entwickeln", erklärt Thomasson. Erste konkrete Ergebnisse aus diesem MEDEA+- Projekt erwartet Thomasson zur Jahresmitte 2002.

Multifunktionskarten

Der große Markttrend geht somit zu Multifunktionskarten, wobei sich eine offene Java-Plattform, wie sie von ST-Microelectronics bereits mit der 32-bit-Plattform SmartJ im Frühjahr 2000 vorgestellt wurde (siehe *elektronik industrie* 5/2000, Seite 96ff), auf breiter Front durch zu setzen scheint. Immerhin arbeiteten Dataquest zufolge bereits 24 Prozent aller im Jahr 2000 ausgelieferten SIM-Karten für Handies auf Basis der Java-Card Technologie von Sun. Um die einzelnen Anwendungen innerhalb von Multifunktionskarten zu bedienen, muss auch der Speicherplatz auf den Karten erheblich ansteigen. Die folgenden Smartcard-Produktneuheiten verfügen denn auch über erheblich mehr Speicherplatz als die High-End-Produkte Ende des Jahres 2000.

Nach Ansicht von Anoop Ubhey, Smartcard-Spezialist bei Frost & Sullivan, müssen die Anbieter (vor allem die Karten-Integratoren bzw. Systemanbieter jenseits des Chips) ihr Produktspektrum erweitern, da ihr Erfolg zunehmend von der Fähigkeit abhänge, umfassende und integrierte Lösungen an zu bieten. Dabei gehe es auch um höhere Sicherheit, größere Benutzerfreundlichkeit und besseren Service. Als Beispiel für die stärkere Orientierung auf Komplettlösungen nennt Anoop Ubhey die multifunktionalen Management-Tools „4Most" von Oberthur, die Kartenaussteller in die Lage versetzen, Anwendungen über das Internet hinzuzufügen, zu ändern oder zu löschen.

Auf der IC-Seite kündigte Philips Semiconductors vor kurzem einen 16-bit-Smartcard-Chip namens SmartXA in der zweiten Generation an, den Gemplus als Basis für seine JavaCard genannte kontaktlose Multi-Applikationsplattform nutzen wird.

HiPerSmart nennt Philips Semiconductors die erste 32-bit-Smartcard-Plattform, die auf der SmartMIPS-Architektur von MIPS Technologies basiert. Sie verfügt gegenüber Vorgänger-Generationen über erweiterte Speicher- und Sicherheitsfunktionen für hochvolumig hergestellte Mehrzweckkarten in den Bereichen Banking, e-Business und 3G-Mobilfunk.

„Die HiPerSmart-Plattform bietet zusätzliche Sicherheitsfunktionen einschließlich Verschlüsselungs-Coprozessoren für DES/AES und PKI und unterstützt die einfache Implementierung virtueller Maschinen wie zum Beispiel Java", erklärt Reinhard Kalla, Business Line Manager Chipcards in der Business Unit Identification bei Philips Semiconductors.

Während MIPS bei der Ankündigung von SmartMIPS bekräftigte, dass einige zusätzliche Befehle innerhalb der Architektur zur Abarbeitung von Kryptographie-Funktionen ausreichen (siehe *elektronik industrie* 6/2001, Seite 58), setzt Philips Semiconductors jedoch lieber auf einen Krypto-Coprozessor als Ergänzung zu SmartMIPS. Neben einer für Mehrfach-Applikationen geeigneten MMU ist bei den technischen Daten von HiPerSmart besonders die Fähigkeit her-

Neben Anwendungen wie Pay-TV und SIM-Karten für Mobiltelefonen gehören die Bereiche Banking und (Internet-)Zugangssysteme zu den wichtigsten Anwendungen von Smartcards

Grafik: STMicroelectronics

vor zu heben, dass die Chips mit Betriebsspannungen zwischen 1,6 V und 5,5 V laufen. Gemplus hat bereits angekündigt, HiPerSmart bei seinen 32-bit-Smartcards der nächsten Generation mit ein zu setzen.

Reinhard Kalla betont, dass die HiPerSmart-Plattform für die Verwendung in Chipkarten und in anderen Gehäusen wie z. B. USB-Tokens entworfen wurde. Kalla weiter: „Da der Markt nach immer größeren Speicherkapazitäten verlangt, bietet der P9SC128, das erste auf der HiPerSmart-Plattform basierende Produkt, insgesamt 64 KByte Flash, 64 KByte EEPROM, 256 KByte ROM und 7 KByte RAM."

STMicroelectronics hat seine aus multiapplikations-fähigen Smartcard-Mikrocontrollern mit erhöhtem Sicherheitsniveau bestehende Produktfamilie ST19 um drei neue Bauelemente erweitert. So ist der mit 96 KByte ROM, 34 KByte EEPROM und 4 KByte RAM ausgestattete ST19XR34 auch mit einem 1.088-Bit-MAP (Modular Arithmetic Processor) für die Public-Key-Kryptographie sowie mit einer ISO-14443-B-gemäßen HF-Schnittstelle für den kontaktlosen Betrieb ausgestattet. Die beiden anderen Varianten bieten vor allem zusätzliche Speicher-Konfigurationen.

„Mit ihren inzwischen über einem Dutzend verschiedenen Ausführungen ist die ST19-Familie ausgezeichnet für Smartcard-Applikationen wie zum Beispiel JavaCard mit hohen Sicherheitsanforderungen geeignet", konstatiert Hajo Brück, Manager in der Smart Cards & Secure Solutions Business Unit bei ST-Microelectronics. Potenzielle Anwendungen sieht Brück vor allem in den Bereichen Datenspeicherung, Banking- und Finanz-Applikationen, Gesundheitswesen, persönliche Identifikation, geschützte Terminals, Telekommunikation, Verkehrsmittel, Zugangskontrolle und Pay-TV.

Als Flaggschiff der ST19-Familie bietet der ST19XR34 neben Hochsicherheits-Funktionen auch eine kontaktlose Schnittstelle. Mit seinem MAP und dem eingebauten DES-Beschleuniger für Public-Key- und Secret-Key-Algorithmen soll der auf einem 1.088-bit-Prozessor basierende und mit einer Bibliothek asymmetrischer Funktionen arbeitende, RSA-fähige Chip dem Designer die Eigenentwicklung der First-Layer-Funktionen ersparen.

Zu den Firmware-Funktionen gehören schnelle, modulare Multiplikationen, Quadrierung, modulare Potenzierung (mit oder ohne Chinese Remainder Theorem), Erzeugung sowie Auswertung von RSA- und DSA-Signaturen sowie weitere Berechnungen an Operanden mit einer per Software selektierbaren Länge bis zu 2.176 bit. Der DES-Beschleuniger arbeitet mit einer im ROM abgelegten Bibliothek symmetrischer Algorithmen, zu denen DES-, Triple-DES-, DESX- und CBC-Chaining-Mode-Berechnungen gehören.

„Der ST19XR34 ist außerdem der leistungsfähigste Mikrocontroller für den kontaktlosen Betrieb", führt Hajo Brück weiter aus. „Er verfügt hierfür über eine ISO-14443-B-gemäße HF-Schnittstelle für den bidirektionalen Datentransfer mit bis zu 424 Kbit/s. Dabei arbeitet das Interface mit einer Trägerfrequenz von 13,56 MHz und erreicht mit 10% Amplitudenmodulation in Senderichtung sowie BPSK-NRZ-Modulation in Empfangsrichtung eine hohe Übertragungsrate."

Die mit einer Spannung von 3 V ±10% betriebene HF-Schnittstelle nutzt eine eingebaute Bibliothek mit 14443-B-kompatiblen Softwarefunktionen zur Kommunikation mit dem Lesegerät. Zu den weiteren zentralen Funktionen und Features des ST19XR34 gehören die im Interesse maximaler Sicherheit vollständig intern ausgeführte Schlüsselgenerierung, der 128 Byte große OTP-Speicher (One-Time Programmable), die drei interrupt-fähigen 8-bit-Timer, ein serieller I/O-Port sowie die bis zu 10 MHz betragende interne Arbeitsfrequenz.

Bei den gemeinsamen Hochsicherheits-Features und -Funktionen der drei neuen Bauelemente handelt es sich um Sicherheits-Firewalls für die Speicher, den DES-Beschleuniger und – im Falle des ST19XR34 – den MAP. Einheitlich sind

Smartcard für UMTS

Auf dem 3GSM World Congress in Cannes kündigte Infineon Technologies seinen neusten Sicherheits-Controller 88S (SLE88CX642S) an, der speziell zum Einsatz in SIM-Karten für GSM- und UMTS-Telefone entwickelt wurde.

Da gemäß einer aktuellen Marktprojektion der Credit Suisse First Bosten der Weltmarkt für mobile Endgeräte, die in diesen Netzen benutzt werden, bis 2003 auf 397 Millionen Stück anwachsen soll, ergibt sich für den Chip ein beachtliches Marktpotential.

Die Speicherkonfiguration wurde speziell auf die Bedürfnisse von GSM zugeschnitten: 192 KByte ROM, 72 KByte EEPROM und 6 KByte RAM ermöglichen auch die Speicherung von Enhanced-SMS-Nachrichten, größeren eMails etc.

Die Sicherheits-Features entsprechen der im Hauptartikel beschriebenen 88er-Architektur und der Platform Support Layer ist ebenfalls lieferbar. Das neue IC arbeitet mit Taktfrequenzen bis 33 MHz bei Betriebsspannungen zwischen 1,8 V und 5,0 V entsprechend den ETSI-Spezifikationen.

auch die EEPROM-Flash-Programmierung mit Beständigkeit für 100 000 bis 500.000 Lösch-Schreib-Zyklen, das Takt-Management sowie die Sensoren für Taktfrequenz und Spannung. Jeder Chip ist überdies mit einer eindeutigen Seriennummer versehen. Einzelbit-Fehler in einem Byte lassen sich im integrierten EEPROM korrigieren. Die MCU-Plattform ST19 ist gemäß ISO 15408 nach den Common Criteria auf der Stufe EAL4+ zertifiziert. Die Bauelemente sind beständig gegen elektrostatische Entladungen bis über 5 000 V. Zur Entwicklung von Software und Firmware bietet STMicroelectronics das unter Windows NT und Windows 98 lauffähige Entwicklungssystem ST19-HDSX an, aber auch ein C/C++-Compiler, ein Debugger und ein Simulator sind lieferbar. Als erstes Mitglied der 88-Familie von Infineon Technologies gibt es jetzt den SLE88CX720P, der über eine spezielle VML-Beschleunigung (VML_ Virtual Machine Language) verfügt und so für die schnellere Ausführung von JavaSC-Anwendungessoftware und anderen stackorientierten Programmiersprachen sorgt. Der Chip basiert auf einer 32-bit-RISC-CPU und arbeitet mit Taktfrequenzen von bis zu 66 MHz.

Die 88-Familie basiert auf einer Workstation-ähnlichen Core-Architektur mit Cache-Speichern für Daten und Befehlen zur schnellen Programmausführung durch das Prefetching (vorausschauendes Laden von Befehlen aus dem Speichern) von Befehlen. Die Virtual-Machine-Beschleunigung unterstützt alle gängigen Chipkarten-Sprachen wie JavaSC, MultOS und Windows Powered Smart Cards. Dabei ist die Chip-Architektur darauf optimiert, verschiedene Anwendungen parallel zu verarbeiten und Peripherie-Funktionen wie die externe Kommunikation über die integrierte serielle UART-Schnittstelle auszuführen.

Neben der nach Angaben von Dr. Hermann Eul (Leiter des Geschäftsbereichs Sicherheits- & Chipkarten-ICs bei Infineon Technologies) „branchenweit leistungsstärksten DPA/SPA-Funktionalität“ (Differential Power Analysis / Simple Power Analysis; Analysen der Verlustleistungsaufnahme) verfügt die MMU des Chips auch über „Hardware-Firewalls, um die Anwendungen und sonstige System-Software sicher und zuverlässig gegeneinander abzugrenzen“ (Dr. Eul). Die integrierten Krypto-Coprozessoren ermöglichen die Berechnung von symmetrischen und asymmetrischen Algorithmen wie DES, Triple-DES, RSA sowie die von elliptischen Kurven. Dabei berechnet das IC RSA-Algorithmen mit Schlüssellängen von 1024 bit innerhalb von weniger als 65 ms ohne CRT (Chinese Remainder Theorem). Auf dem Chip des für Versorgungsspannungen von 1,8 V bis 5 V ausgelegten SLE88CX720P befinden sich auch 240 KByte ROM, 80 KByte EEPROM und 8 KByte RAM. Mit dem Platform Support Layer (PSL) stellt Infineon einen kompletten Satz an Hardware-Treibern für alle Peripherie-Elemente sowie eine Krypto-Bibliothek zur Verfügung.

Ebenfalls auf Multifunktionskarten setzt Sharp Microelectronics mit einem Smartcard-IC, das neben einem kryptographischen Coprozessor auch einen in der Hardware implementierten Zufallszahlen-Generator enthält. Das Nachladen von Applikationen ist auch unter Java möglich – bei Bedarf sogar kontaktlos. Herausragendes Feature dieses bereits in Japan im Rahmen von Pilotprojekten eingesetzten ICs ist seine Flash-Speicherkapazität von 1 MByte, was derzeit für Chipkarten absoluter Rekord sein dürfte. An diesen Pilotprojekten in 21 japanischen Städten nehmen 2 Millionen Chipkarten-Anwender teil. Neben der Geld- und der Kreditkartenfunktion dienen diese Smartcards auch als Ausweis- und Zahlkarte für öffentliche Bibliotheken und Nahverkehrszüge.

Auf Grund dieser Erfahrung rechnet sich Sharp auch gute Chancen aus, im Jahr 2003 den Zuschlag zu bekommen, wenn in Japan 120 Millionen Personalausweise durch Chipkarten ersetzt werden sollen. 2004 werden dann auch die Führerscheine der Töchter und Söhne Nippons in der Chipkarte gespeichert. Die Karten sollen neben den Kenndaten des Inhabers unter anderem auch ein Passbild und einen Fingerabdruck enthalten.

ARM hat jetzt sein SecurCore-Portfolio für Smartcards um die Cores SC200 und SC210 erweitert. Der SC200-Core integriert die Jazelle für Java Card Technologie und bietet neue Sicherheitsmerkmale. Jazelle wurde speziell an das Betriebssystem Sun Java Card angepasst. „Die ARM Jazelle Java Beschleunigungstechnologie ermöglicht eine bis zu achtfache Leistungssteigerung gegenüber bestehenden 32-bit-Java-Lösungen“, erläutert Richard York, SecurCore Product Manager von ARM. „Dieses Leistungsniveau konnte bisher mit existierenden 8- und 16-bit Java-Card-Lösungen nicht erreicht werden.“ Die Integration der Jazelle-Technologie in die SC200-Familie erlaubt die direkte Ausführung von Java Card-Bytecode. Um den SC200 Core zu ergänzen, stellte ARM zudem den SC210-Core vor. Dieser beinhaltet alle Merkmale des SC200-Cores, integriert aber zusätzlich einen kryptographischen Beschleuniger, der eine RSA-Verschlüsselung ohne CRT bei 20 MHz in weniger als 100 ms ausführen kann.

320 ARM
321 Frost & Sullivan
322 Infineon Technologies
323 MIPS Technologies
324 Oberthur
325 Philips Semiconductors
326 Sharp Microelectronics
327 STMicroelectronics