Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 77 (1999)

Heft: 11

Artikel: Kryptographie und Smart Cards

Autor: Schmidt, Manfred

DOI: https://doi.org/10.5169/seals-877069

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 20.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Exploration Programmes:
Corporate Technology explores Future Telecommunications

Kryptographie und Smart Cards

Wenn von Verschlüsselung die Rede ist, denken die meisten wohl an Geheimdienste und Spionage. Tatsächlich benutzt heute jeder diese Technologie, wenn er oder sie mobil telefoniert, eine Taxcard benutzt oder Bestellungen per Internet erledigt. In Verbindung mit einer Chipkarte ergeben sich Möglichkeiten, die geeignet scheinen, unseren Alltag tief greifend zu verändern. Vertraute Konzepte wie Geldmünzen, Unterschriften und Schlüssel könnten durch das Duo Verschlüsselung und Chipkarte ersetzt werden. Marktbeobachter rechnen entsprechend mit einem Wachstum des Chipkartenmarktes von 947 Mio. US-$ im Jahr 1996 auf über 5 Mia. US-$ im Jahr 2003 (Quelle: Frost und Sullivan [2]).

The Exploration Programme Mobility, Cards and Security has the following goals:
– define concepts for new security products and products with strong security requirements like for example Financial Services
– contribute to avoid losses due to security breaches and reduce costs by considering security in Swisscom's business processes
– maintain and further develop the security competence centre of Corporate Technology to support, as a Swisscom internal entity, the Business Units in security related topics
With its Exploration Programmes, Corporate Technology is exploring telecommunication technologies and new service possibilities with a long-term view of 2–5 years. Further, the expertise built up in the course of this activity enables active support of business innovation projects.

Vertraute Anwendungen wie GSM oder Pay-TV basieren auf der Kombination von Kryptographie und Smart-Card-Technologie und sind ohne diese nicht denkbar. Swisscom setzt bereits heute eine ganze Reihe von

MANFRED SCHMIDT, BERN

Chipkarten ein, auch wenn diese nicht immer als solche erkennbar sind, wie beispielsweise der LEGIC-Batch, der für die Zugangskontrolle und die Zeiterfassung verwendet wird.

Programme Scenario

The programme is structured along two axes, each one addressing one of the two strategic questions:
– How shall we guarantee the security of Swisscom services and protect them against fraud and malicious actions?
– What are Swisscom's roles and opportunities in future card-based businesses and the associated financial transactions services?

Derjenige Teil des Explorationsprogramms, welcher die erste der im Programmszenario erwähnten strategischen Fragen angeht, wird «defensive Achse» genannt, da hier der Schutz existierender Dienste und das Vermeiden von Verlusten durch bösartige Angreifer im Vordergrund steht. Im Gegensatz dazu bearbeitet die «offensive Achse» des Programms zur Beantwortung der zweiten strategischen Frage Aspekte, welche zu neuen Diensten und Verdienstmöglichkeiten führen sollten. Dabei liegt das Schwergewicht auf Smart Cards und ihren Möglichkeiten für sichere Dienste zugunsten von Swisscom-Kunden.

Dieser Artikel gibt eine Einführung in das Gebiet der Smart Cards; was sie sind, wie sie sich entwickelt haben und was von dieser Technologie in Zukunft erwartet werden kann. Im Zusammenhang mit dem hier behandelten Explorationsprogramm sind Smart Cards als «Sicherheitsmünzen» (security token) von besonderem Interesse. Deshalb wird auch eine kurze Einführung in die Kryptographiealgorithmen gegeben, um die am besten unterstützten Prozesse zeigen zu können.

Im Weiteren werden zunächst die technischen Aspekte der Chipkarten beleuchtet. Nach einer kurzen Einführung in die Verschlüsselung und die Chipkartensoftware werden einige Anwendungen vorgestellt, unter anderem die Idee einer Personal Card Swisscom als Chipkarte.

Smart-Card-Hardware

Einfache Chipkarten, wie die heute verwendeten Taxcards, sind nicht «smart». Diese Karten werden als Memorykarten bezeichnet und verfügen über einen kleinen Speicher sowie eine im ROM eingebrannte logische Schaltung (mask). Eine solche Karte ist billig in der Herstellung (Tabelle 1) und wird nach «Verbrauch» weggeworfen. Im Gegensatz dazu wird unter einer Smart Card im Allgemeinen eine Chipkarte mit Mikroprozessor verstanden. Somit können Smart Cards auch als «Miniaturcomputer ohne Mensch-Maschinen-Interface» charakterisiert werden. Einfache Chipkarten, wie zum Beispiel die Taxcard, verfügen dagegen lediglich über Speicher und eine Ein-/Ausgabe-Schnittstelle. In der Regel dient eine Plastikkarte als Chipträger. Andere Trägermedien wie Ringe oder Uhren sind ebenfalls möglich. So hat der Erfinder der elektronischen Geldbörse, Roland Moreno, ursprünglich an einen Ring gedacht.

Die physischen Eigenschaften der Chipkarte und die Anordnung des Chips auf der Karte sind im ISO-Standard 7816 bestimmt. Die Kosten und die enormen physischen Anforderungen, denen eine solche Karte klaglos und zuverlässig genügen muss, bedingen eine sehr kleine Siliziumfläche (< 25 mm^2). Auf dieser Fläche untergebracht sind der Mikroprozessor, die Ein-/Ausgabeeinheit und Speicher, aufgeteilt auf RAM, ROM und EEPROM (Electrical Erasable Programmable Memory) (Bild 1). Der Mikroprozessor hat in der Regel eine Busbreite von 8 Bit bei einer Taktrate von 1–10 MHz. Bis vor ein oder zwei Jahren war der Speicherplatz auf einer Smart Card ein kostbares Gut und Entwickler bemühten sich buchstäblich um jedes Bit. Heute umfasst der Speicher einer Smart Card in der Regel 4–32 kByte (zum Vergleich: eine maschinenbeschriebene DIN-A4-Seite enthält etwa 1–2 kByte). Damit ist die Rechenleistung einer Smart Card vergleichbar mit

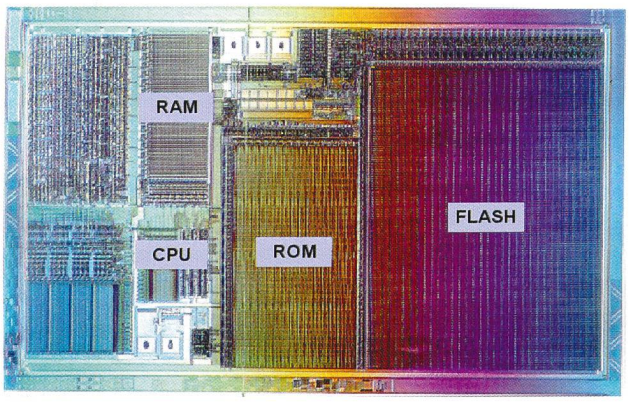

Bild 1. Fotografie eines Smart-Card-Mikroprozessors (Gemplus).

jener des ersten IBM-PC. Die Ein- und Ausgabe erfolgt über einen seriellen Kanal half-duplex, bei einer Übertragungsrate von etwa 9,6 kbit/s. Diese Miniaturcomputer verfügen aber weder über einen eigenen Taktgeber noch über eine eigene Stromversorgung. Beides muss durch ein Terminal bereitgestellt werden.
Im Gegensatz zu einer Magnetstreifenkarte wird bei einer Smart Card jeder Zugriff auf den Speicherinhalt durch den Mikroprozessor kontrolliert. Daher ist es insbesondere nicht möglich, den Speicherinhalt zu kopieren, und es können auch vertrauliche Informationen auf der Karte gespeichert werden. Mit der wachsenden Bedeutung von Smart Cards steigen allerdings auch im Bereich der Hardwaresicherheit die Ansprüche an die Hersteller. Um den Chip vor unbefugtem Öffnen zu schützen, versieht etwa der Kartenhersteller Schlumberger bei einigen seiner Kartenprodukte den Chip mit einer Folie, die sich nicht entfernen lässt, ohne den Chip zu zerstören. Andere Hersteller versuchen durch ein sehr unregelmässiges Speicher-Lay-out (scrambling), das gezielte Auslesen einzelner Speicherzellen zu verhindern.
Smart Cards, die vor allem dem Zweck dienen, kryptographische Algorithmen auszuführen, sind oft mit einem spezialisierten Co-Prozessor ausgerüstet, der diese Verfahren hardwaremässig unterstützt. Während die Rechenzeit damit drastisch vermindert werden kann, entsteht mit dem Datenaustausch zwischen den Prozessoren jedoch ein neuer Angriffspunkt.
Für Anwendungen, die einen schnellen Lesevorgang bedingen, vor allem beim öffentlichen Verkehr oder bei der Zugangskontrolle, ist eine kontaktlose Chipkarte besonders geeignet. Durch induktive Kopplung können Stromversorgung und Datenaustausch bei einem Abstand von wenigen Millimetern bis zu einigen Metern realisiert werden.

Smart-Card-Software

Im Bestreben, den raren Speicherplatz auf einer Smart Card effizient auszunutzen, haben Chipkartenhersteller verschiedene proprietäre Betriebssysteme entwickelt, die den Speicherplatz optimal ausnutzen. Dabei sind Sicherheit, Geschwindigkeit und Stabilität die entscheidenden Herausforderungen. Diese Betriebssysteme ermöglichen die Datenübertragung von und zur Karte, Speichermanagement und die sichere Ausführung kryptographischer Algorithmen. Diese elementaren Funktionen sind über ein API (Application Programming Interface) dem Programmierer zugänglich.
Neu bietet sich vor allem für Multiapplikationskarten, das heisst Karten, auf denen verschiedene Anwendungen gleichzeitig vorhanden sind (etwa eine elektronische Geldbörse und eine Kreditkartenapplikation), Java als universelle Programmiersprache an. Durch ein zusätzliches Softwarepaket, die Java Card Virtual Machine (JCVM), ist es möglich, denselben Programmcode und dasselbe API für Karten verschiedener Hersteller zu verwenden (write once, run anywhere) und damit den Nachteil proprietärer Betriebssysteme teilweise auszugleichen. Zusätzliche Sicherheitsmechanismen dieser objektorientierten Programmiersprache unterstützen die Sicherheit des Smart-Card-Systems.
Die hervorragenden ökonomischen Perspektiven von Smart Cards haben auch Miscrosoft auf den Plan gerufen: Für 1999 wurde eine Smart-Card-Version des Betriebssystems Windows CE angekündigt.

Verschlüsselung

Neben ihrer Funktion als Datenspeicher wurden Smart Cards bereits früh als Verschlüsselungsmodule verwendet. Sie sind dazu besonders geeignet, da alle Berechnungen innerhalb der Smart Card durchgeführt werden können, also Programme und Schlüssel niemals die Karte verlassen müssen.
Kryptographische Algorithmen werden im Allgemeinen für zwei Zwecke verwendet: zum einen zur Sicherung der Vertraulichkeit von Information und zum zweiten zur Sicherung der Integrität. Diese beiden Ziele sind unabhängig voneinander. Während Vertraulichkeit bedeutet, dass nur bestimmte Personen Zugang zu der geschützten Information erhalten sollen, bedeutet Integrität den Schutz vor Verfälschung der Information.
Es mag zunächst verwundern, dass die gebräuchlichsten Verschlüsselungsalgorithmen allgemein bekannt und veröffentlicht sind. Die Idee dahinter wird als Kerckhoff-Prinzip bezeichnet: Die Sicherheit eines Verschlüsselungsalgorithmus sollte allein durch die Vertraulichkeit des Schlüssels, nicht des Algorithmus gewährleistet sein.
Es ist zunächst leicht, ein Verschlüsselungssystem anzugeben, dass nicht gebrochen werden kann: der One-Time-Pad (Bild 2). Dazu muss allerdings der geheime Schlüssel ebenso lang sein, wie die zu verschlüsselnde Nachricht. Stattdessen werden Algorithmen verwendet, deren Sicherheit relativ ist. So gilt ein Verschlüsselungssystem als «praktisch sicher», wenn es selbst bei enormem Aufwand mehrere Jahre dauern würde, um die Verschlüsselung rückgängig zu machen. Selbstverständlich liegt diesen Aussagen immer der gegenwärtige Stand der Technik zugrunde. Grosse Fortschritte in der mathematischen Zahlentheorie oder in der Informationstechnik können diese Annahmen leicht entwerten.

One-Time-Pad

Verausgesetzt der Schlüssel ist geheim und wird nur ein einziges Mal benutzt, ist das folgende Verfahren zu 100% sicher: Der Schlüssel besteht aus einer möglichst zufälligen Bitfolge; die Nachricht wird ebenfalls als Folge aus Nullen und Einsen dargestellt.
Zur Verschlüsselung werden der Schlüssel und die Nachricht ohne Übertrag binär addiert (1+=0!) und das Ergebnis versendet.

```
  1001 0111 Nachricht
+ 1101 0011 Schlüssel
  0100 0100 verschlüsselte Nachricht (wird übertragen)
```

Zur Entschlüsselung wird mit dem Ergebnis genauso verfahren und der Schlüssel «kürzt sich weg»:

```
  0100 0100 verschlüsselte Nachricht (empfangen)
+ 1101 0011 Schlüssel
  1001 0111 Nachricht
```

Bild 2. Sichere Verschlüsselung: One-Time-Pad.

Verschlüsselungsalgorithmen werden in symmetrische (secret key) und asymmetrische Algorithmen (public key) unterteilt. Symmetrische Algorithmen verwenden denselben vertraulichen Schlüssel zur Verschlüsselung wie zur Entschlüsselung. Der bekannteste symmetrische Verschlüsselungsalgorithmus ist DES (Data Encryption Standard). Ein Schlüssel besteht hier aus einem 64-bit-Wort. Da darin acht Parity-Bits enthalten sind, sind damit insgesamt $2^{56}=7{,}2\times10^{16}$ verschiedene Schlüssel möglich. DES verschlüsselt Blöcke von 8 Byte Länge. Im einfachsten Fall (Electronic Code Book, ECB) wird die zu verschlüsselnde Nachricht in Blöcke à 8 Byte zerteilt und jeder dieser Blöcke einzeln mittels DES verschlüsselt, wobei eventuell die Nachricht mit Nullen aufgefüllt wird, damit die Länge ein Vielfaches von 8 Byte beträgt (padding). Die resultierenden Blöcke sind ebenfalls wieder 8 Byte lang; die Länge der Nachricht verändert sich also nicht. Die Entschlüsselung funktioniert nun genauso: Durch zweimaliges Verschlüsseln ergibt sich wieder die ursprüngliche Nachricht. Obwohl in der Praxis sehr häufig angewandt, ist die Beschränkung der Schlüssellänge bei DES auf 56 Bit ein Nachteil, der sich aufgrund der Fortschritte in der Halbleitertechnologie in Zukunft verschärfen wird.

Erst 1976 wurde die Idee eines asymmetrischen Verschlüsselungsalgorithmus vorgestellt [4]. Zwei Jahre danach stellten R.L. Rivest, A. Shamir und L. Adleman einen solchen Algorithmus vor, der nach seinen Erfindern benannt (RSA-Algorithmus) und bis heute das verbreitetste Verfahren dieser Art ist. Dabei verfügt jeder Benutzer über ein Schlüsselpaar, von dem einer, der Public Key, öffentlich bekannt ist – etwa durch Hinterlegung in einem öffentlich lesbaren Verzeichnis –, während der zweite, der Private Key, geheim bleibt. Nachrichten, die mit einem der beiden verschlüsselt worden sind, können nur mit dem passenden Gegenstück entschlüsselt werden.

Dieser Ansatz eröffnet die Möglichkeit der eindeutigen Identifikation des Empfängers oder des Absenders einer verschlüsselten Nachricht. Im ersten Fall wird eine Nachricht mit dem Public Key des beabsichtigten Empfängers chiffriert, sodass nur der Besitzer des zugehörigen Private Keys die Nachricht entschlüsseln kann. Diese Funktion entspricht der eines Briefkastens mit Schloss: Jeder kann einen Brief einwerfen, aber nur der Inhaber des Schlüssels kann die Nachrichten lesen. Im zweiten Fall wird die Nachricht mit dem Private Key des Absenders verschlüsselt. Jeder Empfänger kann diese Nachricht mit dem Public Key entschlüsseln und so den Absender indentifizieren. Diese Funktion entspricht einem verschlossenen Schaukasten: Jeder kann den Inhalt sehen, aber nur der Eigentümer des Schlüssels kann eine Nachricht anbringen. Da asymmetrische Algorithmen rechenintensiver sind als symmetrische, werden oft beide Verfahren gemeinsam verwendet: Zuerst wird mit einem asymmetrischen Verfahren ein vertraulicher Schlüssel übermittelt, dann wird dieser Schlüssel für die symmetrische Verschlüsselung der Daten verwendet (Bild 3).

Bild 4. Mögliche Anwendung: Smart Card als Personal Card Swisscom.

Wenn tatsächlich nur die Identifikation des Absenders und die Unverfälschtheit der Nachricht beabsichtigt sind, ist es nicht nötig, die gesamte Nachricht zu verschlüsseln. Mit den beschränkten Ressourcen einer Smart Card kann das für umfangreiche Dokument eine Weile dauern. Stattdessen wird das Dokument zunächst auf eine feste Länge (in der Regel 160 Bytes) komprimiert. Diese Kompression muss nicht umkehrbar sein und eine kurze Überlegung zeigt, dass das bei einer festen Länge auch nicht immer möglich sein kann. Algorithmen, die auf diese Art einen Fingerabdruck eines Dokuments erzeugen, werden Hash- oder auch Einwegfunktionen genannt. Wesentlich ist dabei zum einen, dass der Inhalt des Dokuments nicht verändert werden kann, ohne auch den Fingerabdruck oder Hashwert zu verändern, und zweitens, dass es trotz bekannter Funktion (!) praktisch unmöglich ist, aus dem Hashwert das Original zu rekonstruieren (daher auch der Name Einwegfunktion). Gebräuchliche Hashfunktionen sind SHA-1, MD4, und MD5. Dieser «Fingerabdruck» wird nun – statt der Nachricht – mit dem Private Key des Absenders verschlüsselt und an die Nachricht angehängt. Sofern die verwendete Hashfunktion angegeben ist und der Public Key bekannt ist, kann jeder Empfänger der Nachricht überprüfen, ob genau diese Nachricht von genau diesem Absender stammt oder nicht. Ein solcher Anhang heisst digitale Signatur. Zur digitalen Signatur wird also der Private Key zur Verschlüsse-

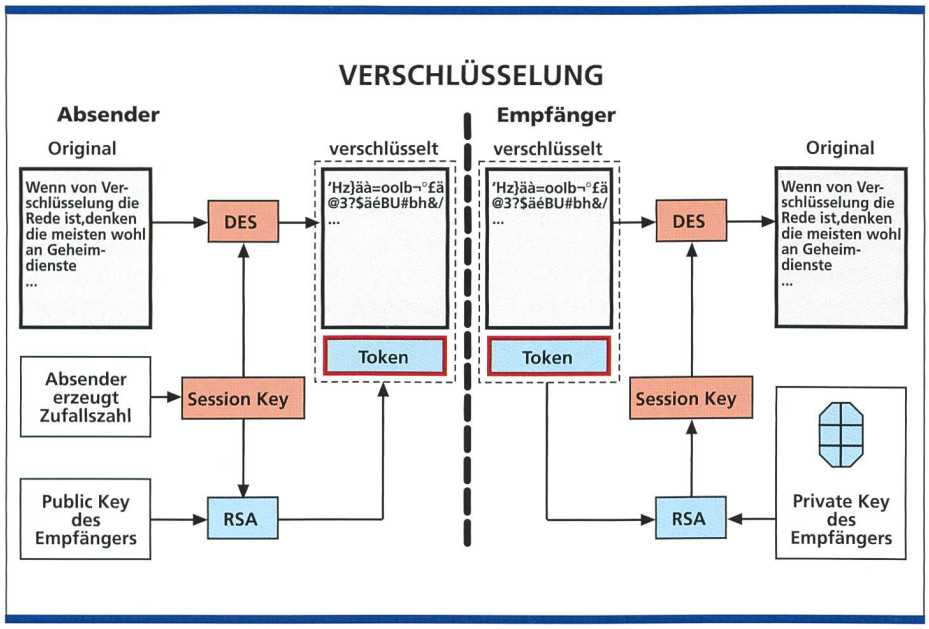

Bild 3. Kombination von asymmetrischer und symmetrischer Verschlüsselung: Da die Verschlüsselung mit asymmetrischen Algorithmen sehr rechenintensiv ist und viel Zeit braucht, wird auf diese Weise lediglich ein geheimer Schlüssel vereinbart, der dann für die schnellere, symmetrische Verschlüsselung benutzt wird.

lung des Hashwertes benutzt, wodurch nicht Vertraulichkeit, sondern Integrität erreicht wird.
Es ist schliesslich ebenfalls möglich, sich mittels Private Key sicher über ein offenes Netzwerk zu identifizieren (Challenge/Response-Verfahren): Dazu wird von der Seite, die eine Identifikation wünscht, eine Zufallszahl erzeugt und übermittelt (challenge); diese wird von der zu identifizierenden Person mittels Private Key verschlüsselt und zurückgesendet (response). Eine Überprüfung erfolgt dann mit dem zugehörigen Public Key. Hierbei ist es wesentlich, dass es sich um eine nicht vorhersagbare Zahl handelt, da sonst eine alte Nachricht abgefangen und eventuell wieder verwendet werden kann.
Die Glaubwürdigkeit einer solchen digitalen Unterschrift wird durch zwei Faktoren bestimmt: die Geheimhaltung des Private Keys und die Echtheit des public keys – der Empfänger muss sicher sein, dass der Public Key wirklich zu dem angegebenen Absender gehört.
Für den ersten Zweck sind Smart Cards wie geschaffen: Sie bieten nicht nur die Möglichkeit, Daten sicher und portabel aufzubewahren, sondern sind auch dazu in der Lage, eine Verschlüsselung in der Karte durchzuführen, sodass der Private Key die Karte niemals verlassen muss. Es ist nicht einmal nötig, dass der Absender seinen eigenen Private Key kennt.
Um zweitens die Echtheit des Public Key zu garantieren, kann ein vertrauenswürdiger Vermittler, eine so genannte Zertifizierungsstelle (Certification Authority, CA) verwendet werden. Die Stelle verwaltet die public keys ihrer Kunden und gibt sogenannte Zertifikate aus, die mindestens den Public Key und den Namen des Inhabers beinhalten und durch die CA digital unterschrieben sind. Das Format eines solchen Zertifikats ist im Standard X.509 festgelegt. Durch die Standardisierung der Zertifikate kann dasselbe Zertifikat für verschiedene Zugriffsmethoden (z.B. Internet, GSM Dualslot, Screenphone, Payphone) zur Authentisierung eingesetzt werden. Weitere Aufgaben der CA sind der Rückruf ungültiger Schlüssel. In der Schweiz kann diese Aufgabe von Swisskey AG wahrgenommen werden, an der Swisscom und die Telekurs Group massgeblich beteiligt sind.
Auf einer solchen Public-Key-Infrastruktur (PKI) basiert SET (Secure Electronic Transaction). Diese Spezifikation wurde von Mastercard und Visa entwickelt und 1997 veröffentlicht, um auf sichere Weise das Bezahlen über offene Netze wie das Internet zu ermöglichen. Bei SET erhält jeder Teilnehmer (Kunde, Händler und Bank) zwei Zertifikate, je eins zur digitalen Unterschrift und zur Schlüsselübergabe. Mit diesen Zertifikaten authentifizieren sich dann alle beteiligten Parteien und alle Übermittlungen werden chiffriert. Die Ausgabe der Zertifikate wird dabei über einen «Vertrauensbaum» realisiert: Ausgehend von einem globalen Root Key werden die Zertifikate der Kartenprodukte authentisiert, dann auch diejenigen der lokalen CAs und damit schliesslich auch die Zertifikate der Kunden, Händler und beteiligten Finanzinstitute.

Links

SET-Platform:
www.set.ch
JavaCard:
http://java.sun.com/products/javacard/
Smart Cards allgemein:
http://www.unc.edu/cit/guides/irg-35.html
Smart Card for Windows:
http://www.microsoft.com/presspass/features/1998/smartcardbg.htm
DPA-Infos:
http://www.cryptography.com/dpa/technical
The Swiss SmartCard Hackers Association:
http://szene.ch/smartcard/

Schlussfolgerungen: Sicherheit ist relativ

Sicherheit ist relativ, auch bei Smart Cards. Die beiden wesentlichen Angriffsstellen der Hardware von Smart Cards sind erstens die Abwesenheit einer autonomen Stromversorgung und eines Taktgebers und zweitens die Abwesenheit eines eigenen Ein- und Ausgabegeräts. Sofern die verwendeten Algorithmen und der Chip selber bekannt sind, ist es oft möglich, aus dem Stromverbrauch und der Verarbeitungszeit auf die internen Abläufe zu schliessen. Die Veröffentlichung einer solchen Methode (Differential Power Analysis, DPA) im Internet hat einige Aufregung verursacht (http://www.cryptography.com/dpa/technical).
Eine Smart Card ist immer auf ein Terminal bzw. auf einen PC angewiesen. Ob nur die Informationen, die der Benutzer auf seiner Karte wähnt, dort sind, kann er nur mit einem Gerät feststellen, dem er dann ebenfalls trauen muss.
Um diese Angriffspunkte zu beseitigen, wäre es notwendig, den Secure Chip, den eine Smart Card darstellt, durch ein Secure Device zu ersetzen, das neben eigener Stromversorgung und Taktung auch sichere Ein- und Ausgabegeräte beinhaltet. Ein solches Gerät könnte ein Handy oder ein Palmtop sein.

Ausblick: Anwendungen

Personal Card Swisscom
Da Swisscom-Mitarbeiter und -Mitarbeiterinnen oft in Situationen sind, die eine Authentifikation über das Netz (Passwör-

Private Karten	maximale Speicherkapazität	Rechenleistung	Kosten einer Karte	Kosten eines Lesegerätes
Magnetstreifenkarte	140 Bytes	keine	0.20–0.75 $	750 $
Memory Card	1 kByte	keine	1– 2.50 $	500 $
Smart Card	8 kByte	8 und 16 bit cpu	7–15 $	500 $
Optical Memory Cards	4,9 Mbytes	keine	7–12$	3500–4000 $

Tabelle 1. Kostenvergleich Chipkarten (Quelle: Gartner Group).

Literatur

[1] W. Rankl / W. Effing: Smart Card Handbook, Wiley, Chichester, 1997.
[2] Stefan Krempl: Alles auf eine Karte, NZZ vom 6. August 1999.
[3] B. Fastenrath, T. Reiners, S.-H. Wabnitz: Smart is beautiful, iX 9/98.
[4] W. Diffie / M.E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, v. IT-22, n. 6, Nov 1976, pp. 644–654.

ter) oder gegenüber Anlagen nötig machen, liegt die Idee einer smarten Personalkarte nahe (Bild 4). Eine solche Karte würde standardisierte Zertifikate verwenden und wäre mit einem PIN geschützt. Falls jeder PC mit einem entsprechenden Kartenleser ausgestattet wäre, würde damit die lästige Eingabe von Passwörtern entfallen. Passwörter sind nicht nur unbequem für die Benutzer, sondern stellen auch ein Sicherheitsrisiko dar, wenn sie an zugänglichen Stellen notiert werden oder von Dritten abgefangen werden. Dabei löst natürlich die Smart Card nicht alle Probleme, sondern dient einzig als sicherer Ort für die Aufbewahrung der Schlüssel, die dann auch weitere Dienste wie Secure E-Mail oder digitale Signatur ermöglichen.
Gegenwärtig wird im Rahmen von EP4 die Möglichkeit des Secure-Single-Sign-on eruiert und im WARD-Projekt ist die sichere Identifikation mit einer Smart Card gegenüber einem Webserver als Prototyp realisiert worden.

White Card
Die weit gehende Standardisierung der Karten und Terminals kann auch als Chance für den Endkunden begriffen werden. Multiapplikationskarten, die mit Anwendungen geladen werden können, trennen die Applikationssoftware von der (Karten-)Hardware, wie heute beim PC. Dadurch geht die Kontrolle der Karte vom Kartenherausgeber auf den Endkunden über. Ermöglicht wird dies etwa durch den Standard Visa Open Platform, der auf Grundlage von JavaCard das Zusammenspiel von Karte, Terminal und Software vereinheitlicht. Ob sich die Idee einer «weissen Karte», die ein Benutzer als Gefäss für die verschiedenen Applikationen benutzt, am Markt wird durchsetzen können, werden die nächsten Jahre zeigen. 4, 7

Manfred Schmidt *studierte in Dortmund Mathematik und Elektrotechnik, promovierte 1998 an der philosophisch-naturwissenschaftlichen Fakultät der Universität Bern und ist seit 1999 bei Swisscom, CIT-CT-TPM, tätig. Ausser dem Bereich Smart Cards und Sicherheit gilt sein Interesse vor allem dem Data Mining.*

Summary

Mobility, Cards and Security

The combination of cryptography and smart card technology is likely to change our every-day life. Cellular telephony and Pay-TV, e-commerce and access control are just some areas where they are already applied. The article describes this technologies and their teamwork, and gives some insight in future trends of this fascinating field that can be anticipated.

TV-Signale, fertig für LC-Display konvertiert

Sanyo Electric hat nach eigenen Angaben einen Chip entwickelt, der übliche Fernsehsignale (PAL, NTSC, digitale Signale) in Ansteuersignale für LCD umwandelt, beispielsweise ein TV-Signal für 480 Zeilen × 620 Spalten in ein Displaysignal 768×1024 nach XGA-Standard für Flachdisplays. Automatische Gammakorrektur für alle drei Farben (RGB) ist eingebaut, ebenfalls die notwendige Bildkorrektur. Sanyo will den Chip bereits im Weihnachtsgeschäft bei seinen eigenen 15-Zoll-LCD-Fernsehgeräten einsetzen. Das Unternehmen will ihn aber auch am freien Rasterfilm getrennt anbieten, ein Rasterfilm, der als Ganzes bereits siebförmig gelocht ist. Dieser Lochfilm besteht aus einem 1 mm dünnen Substrat von der Grösse 50×60 cm, das rund 170 000 winzige Löcher mit 0,1 mm Durchmesser trägt. Das Substrat besteht aus Keramik und Kunstharz. Die erforderlichen Vias werden dann an den vorgesehenen Stellen wie üblich durchkontaktiert. Löcher, die nicht gebraucht werden, bleiben unbearbeitet. NGK hat gemeinsam mit IBM auf das Verfahren Patente angemeldet. Die Lochfilme sollen im Frühjahr 2000 auf den Markt kommen. Über die Preise war noch nichts zu erfahren.

NGK
Insulators 2-56
Suda-cho, Mizuho-ku
Nagoya-shi, Aichi 467, Japan
Tel. +81-52-872 7171
Fax +81-52-872 7103

Cisco bietet jetzt Paketübertragung von Sprache via Internet

Nachdem Cisco kürzlich seine AVVID-Initiative vorgestellt hatte (Architecture for Voice, Video and Integrated Data), ist das Unternehmen jetzt damit an den Markt gegangen: Ende September wurden diverse Vermittlungsswitches, kleine Router und Rufgateways vorgestellt, mit denen Sprache nach Internetprotokoll übertragen werden kann. Dies steht zunächst Unternehmen zur Verfügung. Es steht aber zu erwarten, dass Serviceprovider sich dessen bedienen werden und die (billige) Internettelefonie auch für den Endverbraucher weiter ausbauen werden.

Cisco Systems Inc.
1360 Willow Rd.
Ste. 201, Menlo Park
CA 94025, USA

SAGEM Der Marktleader in Frankreich

Können Sie's freiHandyg?

MC 850 X

Speziell für Mithörer! Die Freisprecheinrichtung des Sagem MC 850 erlaubt auf Wunsch das Mithören über einen eingebauten Lautsprecher.

Easy-message T9™ dank Worterkennung einfache Meldungseingabe, Dualband, Standby über 150 Stunden, integriertes Daten-/Faxmodem, Vibraalarm, 128g leicht ...

miracom
Tel: 041 768 67 67
www.miracom.com

wireless for you

suisse service

EGTel **Unsere Produkte machen Sie erfolgreich!**

Siemens Hicom® 150E Office

Professionelle Telekommunikations-Systeme für 4 bis 250 Teilnehmer

ISDN*simpel*: Die Systemapparate bieten durch die «drei einfachsten Tasten der Welt» problemlosen Zugriff auf alle Funktionen und fallen durch ihr attraktives Design auf. ISDN*flexibel*: Das innovative Adapterkonzept lässt flexible Anpassungen an der Kommunikations-Infrastruktur zu und bietet Schnittstellen für diverse Geräte. ISDN*portabel*: Leistungsfähige, integrierte Cordless-Lösungen sowie günstige DECT-Erweiterungen werden unterschiedlichen Anforderungen an mobile Kommunikation in Unternehmen gerecht. Moderne Leistungsmerkmale wie Fernwartung und dynamisches Least Cost Routing sowie eine Reihe von Anwenderlösungen runden das breite Leistungsspektrum dieser multifunktionalen Telekommunikations-Systemfamilie ab. (Bitte beachten Sie auch unsere Homepage: www.egtel.ch)

Faxcoupon

Ich interessiere mich für Hicom 150 E Office; bitte informieren Sie mich über meine Einkaufs-Konditionen.

- ☐ Bisher sind wir noch nicht Kunde bei Ihnen; eine Kopie des Handelsregister-Auszugs unserer Firma liegt bei.
- ☐ Wir sind bereits Kunde bei Ihnen.
- ☐ Wir interessieren uns auch für eine EGTel-Mitgliedschaft. Bitte nehmen Sie mit uns Kontakt auf.

Bei uns ist zuständig: _____

Firmenstempel

comtec

EGTel AG Albulastr. 55 CH-8048 Zürich Tel. 01-434 66 66 Fax 01-434 66 67 contact@egtel.ch