An Infineon Technologies Publication

Autumn/2001

s@cure

The Silicon Trust Quarterly Report

Quarterly Focus

Traditional Smart Cards vs. USB Token Security – And the winner is...?

PKI goes Mobile

New Players – New Game.

Secure Licensing

Securing Intellectual Property from Software Piracy

www.silicon-trust.com

Impressum

SECURE - The Silicon Trust Quarterly Report
is a quarterly Silicon Trust program publication,
sponsored by Infineon Technologies AG.

SECURE - The Silicon Trust Quarterly Report
is an Infineon Technologies publication

The Silicon Trust Program Director
Veronica Preysing
Email: veronica.preysing@infineon.com

Infineon Editorial Team
Veronica Preysing (Infineon Technologies)
Florence Raguet (Infineon Technologies)

Magazine Project Development
Krowne Communications GmbH
Munich, Germany

Creative Director/Layout
Stefan Gassner
Email – stefan.gassner@krowne.de

Advertising & Distribution
Karen Brindley
Email – karen.brindley@krowne.de

Printing:
ADM Bozen
Siebeneich-Terlan, Italy

Cover Illustration by Stefan Gassner © 2001

Subscriptions of SECURE – The Silicon Trust Quarterly Report can be obtained at: www.silicon-trust.com

Editorial

Welcome to the Autumn 2001 issue of the "Secure", the Silicon Trust Report. In the midst of the current market downturn, the High Tech Industry needs, more than ever, to take innovative, unconventional steps towards market penetration and customer retention. The decision by Infineon's partners and customers to participate in the Silicon Trust is one of those steps.

Six new Silicon Trust Partners since the last Secure issue prove the relevance of this platform, which now counts players from all security areas, the steepest increase coming from the most traditional of the Hardware Security Sectors: the Smart Card Sector. In this issue of Secure we are challenging the hitherto untouchable position of the Smart Card by introducing and comparing the USB Dongle as a potential alternative. Aladdin, Giesecke & Devrient as well as Infineon are contributing to this Quarterly Focus: **Smart Card vs. USB Dongle.**

Another favorite focus remains to be the latest Biometric Solutions on the market and in this issue we are giving an insight into the possibility of securing Computer Peripherals using Partner Solutions.

For more information, please visit www.silicon-trust.com

Last but not least don't miss out on Calumn Bunney's column. Ferociously independent, he does not hold back with his humorous views on what is happening in the Security Industry.

To keep yourself updated, please subscribe to your free copy of Secure at **www.silicon-trust.com** or by faxing back the Subscription Form in this issue.

Veronica von Preysing

Contents

StarAccount
Secure Internet Banking
Giesecke & Devrient
Cert
Your certified Signature Solution
Giesecke & Devrient

HARDWARE SECURITY – WHAT DOES IT MEAN?
HOW CAN THESE PROBLEMS BE RESOLVED
THE ROLE OF SECURITY AND CHIP CARD ICS

Contents

Who's Who in this Issue.

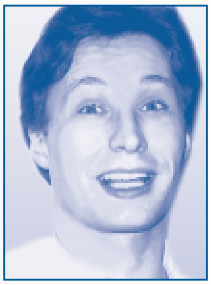
John Atkinson

Giesecke & Devrient

John Atkinson joined G&D in July 2000 as VP Strategy and International Marketing. His team has been focused on the emerging technologies JAVA, PKI, Biometrics, USB Tokens and other form factors. They are also involved in developing strategic alliances and Partnerships with key industry players.

John is a Qualified Electronics Engineer who specialized in the design and development of Communication systems before moving into a more commercial role, firstly as an Applications Engineer and then as a Sales Engineer in the Semiconductor Industry. John moved to the Smart Card Industry in 1993 as he viewed this as a strong potential growth Industry. He has held Management Positions in the Smart Card Industry in the UK, Germany, Singapore and Australia.

Calum Bunney



Calum Bunney is an independent consultant on biometric and authentication technology markets. In 1999 he founded International Biometric & Authentication Consulting Ltd. with offices in the UK and in France, to deliver market and technology development services and information. In the last four years he has authored a number of publications on biometric and autoID technologies, and has presented at and chaired seminars on these topics worldwide. Prior to his involvement with authentication and security technologies he worked for a number of years as a market analyst in the brewing and leisure industries. He holds an honors degree in Philosophy from King's College London.

Monika Bremer

Infineon Technologies AG

Monika Bremer holds the position of "Manager New Markets & Relations e-business" and is based at Infineon Technologies' Head Office, Munich. She started at Infineon in December 2000, and is responsible for e-business in the "New Markets & Relations" – Team. Monika has had many years of experience covering marketing, product- and project management positions in the banking and brokerage area (e.g. HypoVereinsbank).

Dr. Hermann Eul

Infineon Technologies AG

Hermann Eul is a Doctor of Electrical Engineering, who began his career with Siemens' Telecommunications Infrastructure division in 1991, where he had several managing positions in the research and development area. From 1996, he headed various business units in the consumer and telecommunications segments within Siemens Semiconductors. From 1999, he was in charge of the Wireless Communications group's Baseband ICs division. Dr. Eul assumed responsibilities as the head of the Security and Chip Card ICs division from the 1st May 2001.

Charlie Hava

Aladdin Knowledge Systems

Chalie Hava has been working at Aladdin Knowledge Systems for 10 years, starting as a programmer and moving into positions such as Head of HASP R&D team and Product Manager.

Today he holds the position "Solution Partners Program Manager" in the Business Development area. Charlie holds a BSc of Education, Math and Computer Science from Technion Haifa and an MBA from the university of Tel-Aviv.

Harry Knechtel

Secartis

Harry Knechtel is an experienced technical consultant with 5 years of experience in PKI, secure IT infrastructures and security application development. Most recently, Harry fulfilled the role of Chief Security Architect for the Vodafone Secure Framework project, where he was responsible for project managing the delivery of the High Level Design (HLD) documentation. Some of Harry's other relevant accomplishments include the development of a PKI-secured email application for Siemens R&D; consulting and technical implementation of a PKI infrastructure for Daimler Chrysler and the work on a design for governmental PKI system for Asia.

Stefan Kuhn

Siemens AG

Stefan Kuhn is the General Manager/Vice President of Biometrics at Siemens AG. After finishing his studies in Business, Stefan began working at Siemens 10 years ago in the Mobile Communications department, where he was responsible for the worldwide launch of the first "D-Netz" Mobile phone. He then went on to run the retail marketing department for Mobile Communications & ISDN. Five years ago, Stefan began the task of building up sales channels for commercial security products, and in 1999 he led the Fingerprint Project that has since developed into the Biometrics unit of Siemens.

Dr. Peter Laackmann

Infineon Technologies AG

Dr. Peter Laackmann has been developing Hardware and Software components for synchronous and asynchronous Chip Card terminals since 1991. He has written both technical articles and columns for numerous publications covering Chip Card technology, Applications and Security concerns, and between 1993 and 1999 also carried out consultancy work with such television companies as ARD, ZDF, Sat1 and Pro7. After studying data protection/security issues and applications for contactless Chip Cards in the area of "Car Sharing", in 1997 Peter took part in the project called "Die Karte" at the Kuratoriums Deutsche Kartenwirtschaft - going on to complete his PhD at the Christian-Albrechts-Universität in Kiel. He currently manages the Strategy and Concept Engineering department (Security & Chip Card ICs) at Infineon Technologies AG in Munich Germany.

Derek McDermott

Informer Systems Ltd.

After a 15-year career in IT project management with British Leland/ISTEL, Derek McDermott established ISL Informer Systems Ltd. in 1989 as a systems integrator focused on remote access security solutions.

The company has since developed into a security software developer specializing in authentication and in the last 3 years has focused on the development of biometric solutions for the corporate enterprise. ISL is now recognized as a leader in professional solutions for secure authentication.

Magnus Pettersson

Precise Biometrics

Magnus Pettersson M.Sc. EE, Product Manager Embedded Solutions joined Precise Biometrics in February 2000. Magnus was one of the driving forces behind the Precise Match-On-Card technology and has been responsible for the integration of biometrics, smart cards and PKI. Previously, Peter joined the Swedish company CellaVision in 1997, where he worked with image analysis development in medical applications, resulting in two patents. Then in 1998 he joined ABB, and worked for ABB Robotics, Mexico, with installations and as robotic programming instructor. Peter received his Master of Science in Electrical Engineering from the University of Lund in 1997, with an edge in image analysis and computer controlled systems, and has been working in the field ever since.

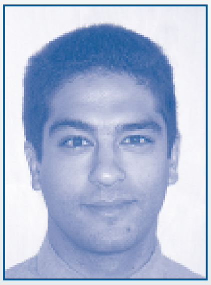
Thomas Röder

Infineon Technologies AG

Thomas Röder joined Siemens Semiconductors in 1998, with 5 years experience in the telecommunications industry. He was previously with Alcatel SEL AG in Stuttgart and Nuremberg, where he led the product technology department for fibreoptic components and the global Quality Office for Alcatel Switching Systems S12. Thomas holds a degree in physics from the University of Stuttgart. Starting at Siemens Semiconductors, Thomas focused on Marketing roles. Since January 2001 at Infineon Technologies AG, he has held the position of Senior Marketing Manager of Security and Chip Card ICs. Currently he is preparing the worldwide market introduction of the new security controller chipset SmartUSB.

Omar Rifaat

Secartis



Omar Rifaat is a Telecoms consultant in Secartis' London office, where he assists customers in understanding the business case for secure mobile applications and then guides them through the technical selection and rollout process. With over three years of experience in PKI and the mobile sector, Omar also has an understanding of the converging mobile, financial and technology markets and seeks to help customers from different backgrounds come together to understand and expliot emerging opportunities.

A Date for Your Diary!

28, 29, 30 November
London, UK
Biometrics 2001

Now in its fourth year, Biometrics 2001 has grown considerably again this year, proving itself as the most important event in Europe. The conference will be multi-stream, with original case studies, information on the fastest moving technologies, government applications, market statistics and other pertinent industry issues. A Privacy Panel has also been arranged, and includes the highly controversial director general of Privacy International – Simon Davies. The first day of the event will comprise of an introductory and advanced biometrics seminar.

To apply for free tickets to the exhibition and to get more information on how to attend this year's cutting edge conference, see our ad in this issue or visit www.biometrics2001.com

Massive biometric project ready to go

Btt September 2001

A potentially massive e-business biometric project is about to be launched, with the backing of some of the world's leading players. Biometric service provider ekey, a division of Voest Alpine, the Austrian steel and engineering company, has announced a project which could involve up to 80,000 fingerprint sensors being deployed in the first half of 2002 alone.

The project involves the use of biometrics in e-banking and e-commerce scenarios and already has the backing of a number of major Austrian banks, Visa, Compaq, IBM and Huber Computer. Each player has had to commit serious money to the venture, with the price of membership starting at DM150,000 (US$67,500).

Following various trials, a large-scale launch is expected next year. Thomas Moser, technical manager at ekey, said: "In the first quarter of 2002 there will be a rollout in Austria. In the third quarter there will be a roll out in Germany and Switzerland and this will be followed by a roll out in the UK and USA in 2003."

The banks have already agreed to pay for the biometric devices, which they will give out to their customers following in-branch enrolment. Moser said that it is looking for a number of sensor manufacturers to provide equipment.

MasterCard to take over Europay

Ctt July/August 2001

MasterCard International and Europay International have agreed in principle to combine their organisations into a single shareholder-owned corporation.

The announcement, made in Munich at Europay's annual membership meeting, is widely assumed to amount to a takeover by MasterCard. Europay banks will form the European region of MasterCard and Europay staff will provide services for the region from their present base in Waterloo, Belgium – although some redundancies are inevitable. Europay's CEO Peter Hoch will report to Bob Selander, MasterCard's CEO.

MasterCard has had a long-standing alliance (since 1970) with Europay, in which it owns a 12.2% share. In addition, MasterCard and Europay each own 50% of the Maestro debit card brand.

Europay contributes to the new company its strength in debit cards and chip cards and in m-commerce (through Europe's lead in mobile phone technology). But Europay's CEO Peter Hoch said that regional scope in the payments industry was no longer good enough.

Micro-processor cards to overtake memory cards by 2005

Ctt July/August 2001

Shipments of micro-processor cards will have overtaken shipments of memory cards by the year 2005, according to the latest forecasts from Eurosmart, the smart card industry's leading trade association.

Lutz Martiny, chairman of Eurosmart, said that the annual rate of growth across the whole smart market over the five years is likely to be in the region of 20% in volume terms. Initially, the shift from memory cards to (high value) microprocessor cards, promises increased revenues. But as volumes of microprocessor cards build up, prices of these too will begin to come down.

Since 1997, the total worldwide market has grown from 900 million cards to an estimated 2015 million in 2001; in other words the industry's shipments have more than doubled in five years. The year 2000 itself was relatively disappointing in volume terms; total shipments of 1,603 million cards showed overall growth of only 12% over the previous year. This was due to slow down in the growth of memory card markets and 'moderate' shipments in emerging sectors, such as health, transport and ID.

Capita to provide smart cards for 16-19 year olds

Ctt July/August 2001

The Capita consultancy group has been selected as the 'preferred bidder' for the UK government contract, worth in excess of £100 million (US$140 million), to develop and deliver the Connexions Card service for 16–19 year old school children in England. The contract will run for an initial seven years, with an option to extend for three years. Capita has emerged as front-runner, ahead of BT Ignite, which has worked on 'Pathfinder' pilots for the Connexions scheme.

The Connexions card will store and monitor benefits available to all young people in further learning. It is projected that the card will be carried by up to 2.4 million young people. The aim is to encourage young people to stay on in learning after the age of 16, and to achieve a worthwhile qualification by the age of 19.

Connexion cards will be rolled out region-by-region beginning in the autumn of this year and should be available across the whole country from autumn 2002.

ActivCard and Precise Biometrics target DOD project

Btt June 2001

Swedish supplier Precise Biometrics and US smart card software developer ActivCard have announced a partnership to provide an on-card biometric verification system operating on the Open platform.

In particular, Precise Biometrics wants to use this partnership to target the US Department of Defence's (DOD) Common Access Card project, where ActivCard has already won a contract to provide software architecture. The DOD has said that on-card matching for its 4.3 million card scheme would be desirable, but not yet made any firm decisions on a supplier.

Japan to issue smart Resident Cards to citizens

Ctt June 2001

The Japanese government is planning to issue its citizens with smart cards as personal ID documents, to be known as Resident Cards. Current plans are to issue between 10 and 50 million people with smart ID cards, beginning in August 2003. The government is already planning a procurement programme for 2001 of between one and three million cards. Smart ID cards will be issued to people only if they are requested, which explains the large variation between projections of possible procurement orders.

New legislation is paving the way for the introduction of the new Resident Cards. An electronic signature law has been passed and the laws governing registration of residents has been amended, in each case to accommodate the issue and use of the smart ID cards. Resident Cards will be issued by local government authorities and will be used primarily as a means of identification for citizens' dealings with public authorities.

The Japanese government has asked European card manufacturers to collaborate in drawing up technical specifications for the Resident Card.

The above news stories are brief excerpts from articles published in Card Technology Today (Ctt) and Biometric Technology Today (Btt). Visit www.compseconline.com for more information.

Introducing the Silicon Trust

With the New Economy growing at an exponential rate, the need for solutions enabling secure E-Commerce, M-Commerce, and banking as well as data and content protection is becoming more critical. Silicon based security is paving the way to make tomorrow's lifestyles secure.

The Silicon Trust – what is it and how do you join?

Partner Mission

The Silicon Trust is a platform created for those businesses utilizing Infineon's Security IC technology and solutions in their end applications. Its primary goal is to develop and enhance market awareness as well as customer acceptance for individual products and solutions developed by the Silicon Trust partners.

The Silicon Trust Vision

The Silicon Trust is an industry platform for silicon-based security technology embracing a unified approach to the marketplace. It intends to become the number-one reference for companies searching for the highest-quality, certified security solutions available across the entire spectrum of products and solutions.

Our Silicon Trust Partners provide the critical link between Infineon and customers with complex projects or significant time constraints. Because our security products serve such a wide variety of applications, opportunities exist for consultants and system integrators with specific vertical market expertise. Silicon Trust Partners add value by writing custom software applications, designing custom hardware, and providing turnkey solutions.

Qualifying for the Silicon Trust

Infineon Technologies aims to work with companies, which provide complementary products or services. You may be eligible to join the Silicon Trust if your company is engaged in:

1. *Hardware or software consulting*
2. *Systems integration*
3. *Third-party products and systems*

Infineon Technologies seeks partners who use Infineon's security products and who want to build a business relationship with Infineon Technologies and other Silicon Trust partners.

The Silicon Trust provides tangible benefits for active members. When evaluating applicants, Infineon Technologies looks for:

- Competency in the area of security products or similar areas.
- A clear business strategy and explanation of how Infineon's security products are a part of your particular solution.
- References from customers who are satisfied with your technical abilities and business practices.
- Sponsorship by the Infineon Technologies representative in your area.

Members of the Silicon Trust

- **ACG**
- **Aladdin**
- **Bioscrypt**
- **CE-Infosys**
- **Datacard**
- **Faktum**
- **G&D**
- **ISL**
- **Jin Woo**
- **Loqware**
- **Omnikey**
- **Pollex**
- **Precise**
- **PSE**
- **SC^2**
- **Secartis**
- **Siemens**
- **Sospita**
- **Startek**
- **Towitoko**
- **Veritouch**

Sales Benefits

- The opportunity to work closely with the Infineon Technologies Worldwide Sales and Technical Support network.

Marketing Benefits

- Listing of your products and services in the Silicon Trust database.
- Publicity of your product announcements and project success in SECURE the Silicon Trust Quarterly Report.
- Participation with and assistance from, Infineon Technologies during key industry events.
- Use of the Silicon Trust Logo for your promotional material.

Technical Benefits

- Partner-only communication channels.
- Discounts on training courses for your developers.
- Access to Infineon Technologies' top application engineers.

For further information visit: www.silicon-trust.com or email contact@silicon-trust.com

Welcome to the Trust

This quarter we would like to welcome the following members to the Silicon Trust. For further information on these companies, please check out their websites.

ACG ...welcome to the smart world

www.acg.de

ACG is a high-tech company in the fast expanding computer chips, Smart Card and contactless technology markets. ACG is positioning itself between the participants along the value-added chain, and it is the intermediary between supply and demand in non-transparent markets. Many suppliers are brought together with many potential buyers.

As a center for products, innovation and information, we have established ourselves in various markets. Our world-wide broker network provides the base for immediate and extensive market penetration. Our thorough knowledge in the field of these electronics products, together with our comprehensive market knowledge are what make our company more than just a brokerage, but a Value Added Reseller.

The ACG sales and product specialists are situated in 34 locations throughout the world so that they are permanently available to our partners for virtually continuous coverage.

Datacard Corporation, doing business as Datacard Group, is a privately held company based in Minnetonka, Minnesota. Worldwide operations include new software development centers in the U.S., the U.K., India and Japan. The company employs more than 1,600 people worldwide and generates annual revenues of more than $300 million.

Datacard provides customers in more than 200 countries with the systems, software and the consultative expertise they need to launch and maintain profitable card programs. Financial institutions, corporations, government agencies, telecommunications companies, transit providers, service bureaus, schools, hospitals and other organizations use Datacard solutions to personalize, issue and manage a variety of financial and identification cards.

Datacard Consult p7 brings more than a decade of advanced Smart Card experience to provide Smart Card consulting and security evaluation services. A full team of mathematicians, cryptographers and Smart Card chip experts provide services including card failure analysis, card evaluation, chip analysis, software development, systems consulting and evaluation consulting.

We offer exceptional expertise in Smart Cards — most notably, multi-application Smart Card programs. In fact, our team currently works with other industry leaders through GlobalPlatform to define interoperability standards for Smart Card technology.

DatacardGroup

www.datacard.com

Giesecke & Devrient

www.gieseckedevrient.com

Giesecke & Devrient (G&D), an internationally operating technology group, is a leading supplier of cards, software and complete multifunctional Smart Card solutions for electronic payment systems and telecommunications. The group also offers banknotes and security documents, brand protection, banknote and security paper and currency automation systems. As a reaction to the rapidly growing global demand for security services for e-business G&D founded Secartis AG in 2000.

ISL (Informer Systems Limited) designs, develops, manufactures and markets software products for the capture and comparison of biometrics, such as fingerprint, and/or Smart Card for security applications including Network Access, Remote Access, Web Access and Database Access. ISL software products provide its customers with the widest and finest choice of biometric hardware technology which includes Sony, Siemens, Cherry, Biolink, Precise Biometrics, BAC, Identix and Ethentica. Established in 1989, ISL headquarters are in Bromsgrove, Worcs, in the UK, and ISL markets its products through authorized reseller and OEM channels. ISL is a leader in biometric security software in the UK and has developed a range of quality, easy to install, easy to support biometric security solutions to address all network and remote access control needs.

ISL Informer Systems Limited

www.informer.co.uk

SECARTIS
eSolutions by Giesecke & Devrient

www.secartis.com

Secartis AG is a service company supporting clients in setting up or migrating to a PKI and in the realization of secure mCommerce and eCommerce applications – from consulting to integration, customization and outsourced operations of secure transaction systems.

Sospita is a core technology company, founded in Norway in 1995. Sospita offers world leading software license protection technology with REAL security. Real security means that the protected parts of the programs are decrypted and run in an environment not accessible to crackers.
Sospita has achieved international patents for its core technology including a US patent awarded in 2001.
The software market totaled 157 Billion USD in 1999 and is growing by approximately 14% per year (source SIIA). 37% of software is pirated on average worldwide each year. This represents a huge market potential for Sospita' software license protection technology. In addition, large potential exists for Sospita's core technology in new software distribution forms over the Internet and new emerging wireless solutions.
Sospita's technology can efficiently be distributed through OEM agreements with international companies who have established distribution and marketing networks.

sospita
Protecting Your Software

www.sospita.com

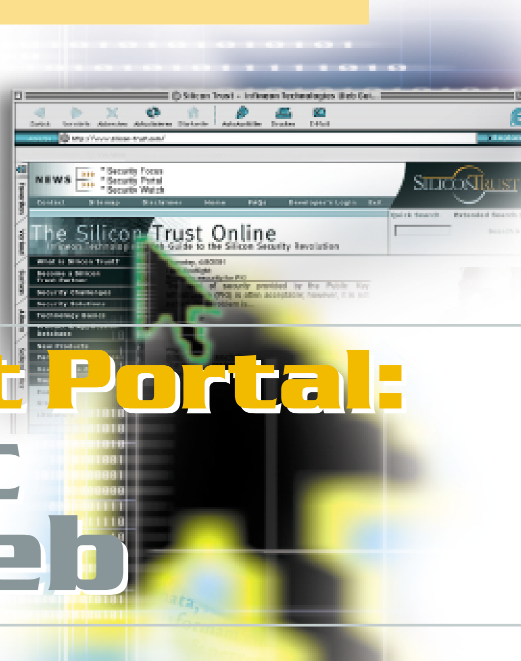
Infineon technologies

www.infineon.com/ident

New Infineon Division joins the Silicon Trust

Following the Security ICs Division and the Chip Card ICs Division, a third Security group will also participate in the Silicon Trust program by inviting their partners to join the Community.
Infineon's Identsystems integrated circuits (ICs) add intelligence about goods to information systems, providing all participants in global supply chains with accurate asset visibility data. Infineon's chips feature flexibility for writing user data to the chip, large memory capacity, and enhanced security features. This makes them particularly well suited for smart label applications in supply chain and logistics management, and in security and control of valuable assets. These applications include RF-based documentation of valuable goods, such as automobiles, and tracking of goods from point of manufacture to point of sale.
With respect to smaller closed systems, it is Infineon's strategy to provide complete Identsystems solutions, beginning with the chip and extending through the process of system design, supplier coordination and implementation

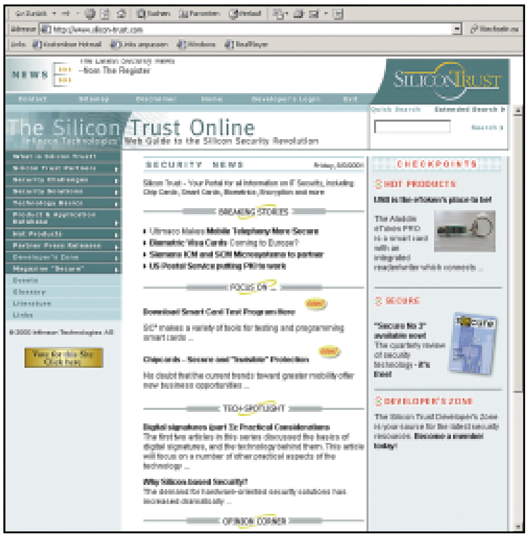
It's been little more than a year since the Silicon Trust (www.silicon-trust.com) went online with a few simple pages presenting the Infineon partner program and industry platform of the same name, initiated shortly beforehand at CeBIT 2000.



The Silicon Trust Portal: SiBaSec on the Web

By .whp. interactive.

The partner program grew at an amazing rate, and several months later, in November 2000 it was time to make the site reflect the extensive array of expertise, technologies and products available from Infineon and the companies it works with.



The Silicon Trust Online

Web Guide to the Silicon Security Revolution

SECURITY NEWS

Silicon Trust - Your Portal for all Information on IT Security, including Chip Cards, Smart Cards, Biometrics, Encryption and more

BREAKING STORIES

- Utimaco Makes Mobile Telephony More Secure
- Biometric Visa Cards Coming to Europe?
- Siemens ICM and SCM Microsystems to partner
- US Postal Service putting PKI to work

FOCUS ON ...

Download Smart Card Test Program Here

Chipcards – Secure and "Invisible" Protection

TECH-SPOTLIGHT

Digital signatures (part 3): Practical Considerations

Why Silicon based Security?

OPINION CORNER

CHECKPOINTS

HOT PRODUCTS

SECURE

"Secure No 3" available now!

DEVELOPER'S ZONE

The relaunch meant a considerable increase in the amount of information available on the web site, offering visitors high-quality reference information on hardware-based security technologies such as biometrics and Smart Cards; crucial background on subjects such as encryption, and articles on a wide range of partner products utilizing the latest technologies.

Today the site continues to grow and expand: Catch security news tidbits every day, check out the 'Tech Spotlight' and 'Security Challenges' sections featuring a series of articles on digital signatures aimed at laypersons as well as decision makers, and two upcoming articles which will cover the latest in security for mobile devices and e-banking. And watch for our improved navigation function, providing even better site transparency.

The Silicon Trust has also coined the term **'SiBaSec'** – **Si**licon-**Ba**sed **Sec**urity – to denote the essential pursuits of the members of this growing industry platform. Planned articles that will be found on the portal site will cover topics such as SiBaSec and Linux, SiBaSec and Academia, and SiBaSec and the Smart Home.

SiBaSec and E-Government

If you haven't already, take a look at the Silicon Trust article on Silicon-Based Security and e-Government. E-Government is a topic, which is becoming increasingly popular; the upcoming Systems 2001 will have its own e-Government area this year. Various local, regional, and national governments as well as citizens and businesses are discovering the blessings of being able to exchange information, handle a wide variety of administrative procedures (registering cars, making address changes, getting birth certificates, paying taxes, and much more), and communicate over the Internet. Especially in this area, however, security must be stringently handled – and of course, hardware- based security is the key to the best security. The article discusses how the Northern German city of Bremen set up a model e-Government program which meets citizen as well as security requirements.

The Silicon Trust portal can be found at: www.silicon-trust.com

The show season is upon us once more. With the Silicon Trust present at more shows and exhibitions than ever before, it is an excellent opportunity for you, the reader, to come and meet with members of the Silicon Trust and discuss your security needs and issues.

Welcome to Show Season

This season, the Silicon Trust will be present at ISSE 2001, London, England; Cartes 2001, Paris, France; Biometrics 2001, London, England; InfoSecurity 2002, London, England and CTST 2002, New Orleans, USA. The Silicon Trust presence will be either through its own partner booths or on booths hosted by Infineon Technologies. If you are also interested in other shows or exhibitions happening within the Security industry, you can find a larger list with details on the Silicon Trust Portal site at www.silicon-trust.com/events/events.htm.

ISSE 2001
www.eema.org/isse/
26th Sept. – 28th Sept. 2001.
QE2 Conference Centre.
London, England

Cartes 2001
www.cartes.com
23rd-25th October 2001
CNIT, Paris, France

Biometrics 2001
www.biometrics2001.com
29th-30th November 2001
London, England

InfoSecurity 2002
www.infosec.co.uk
23rd-25th April 2002
Olympia., London, England

CTST 2002
www.ct-ctst.com/
22nd-25th April 2002
New Orleans, USA

Security Solutions Forum.

The Silicon Trust will also be hosting its second Security Solutions Forum in Munich, Germany in September 2001. This second event is a follow-on from the first event held in February earlier this year. This two-day Partner only event hopes to continue the networking and involvement from partners that was in evidence during the last Security Solutions Forum – a real step forward towards developing a community for Silicon based Security Solutions!

The Marketing/Business Development Tracks, in this Forum, will concentrate upon such issues as terminal security, user authentication and data security, and round-table issues such as ownership of end users, co-op marketing, trend setting and cross-industrial alliances. During the Technical Tracks, Partners have the chance to train each other and Infineon staff on their products and technology, thus ensuring cross-fertilization of knowledge and experience.

Look out for a review of the Forum in SECURE Issue 5.

Recently, the market research institute Dataquest, declared that Infineon Technologies had taken the World's No. 1 spot in the area of Chip Card ICs. What was even more interesting was the fact that this wasn't the first time – but the third time in a row!

SECURE spoke with the new head of the Security and Chip Card ICs group – Dr. Hermann Eul, about Infineon's Chip Card products, their applications and more importantly, what the future holds in store for Chip Card products.

Chip Cards

Applications with a Secure Future

SECURE - What products, technologies and manufacturing processes does Infineon Technologies offer today for Chip Card applications?

Dr. Eul - Since entering the Chip Card arena about a decade ago, Infineon has sold more than four billion Chip Card ICs worldwide. Today, we offer the industry's broadest portfolio of products for Chip Card applications, including both security controllers and security memory ICs for cards as well as for the terminals that read them.

With these ICs for both cards and terminals, we now offer complete chip systems for contactless Chip Card applications, regardless of configuration. In terms of manufacturing processes, Infineon's 66Plus families of 16-bit Chip Card controllers are produced using the most modern 0.22-micrometer technology in the world for Chip Card ICs. In addition, as the world's first manufacturer of Chip Card ICs, we also manufacture a 16-bit security controller with a very large non-volatile EEPROM memory with 64 kilobytes capacity in volume units. Such a memory capacity offers a new dimension of flexibility to mobile communications service providers, allowing network providers to offer numerous extra wireless services including: mobile banking and mobile-commerce functionality within their networks, a heavily enlarged user profile - memorizing a significantly extended number of UMTS abbreviated dialing numbers, infotainment and entertainment services, as well as the possibility to easily and significantly extend these services, even after distribution of the SIM cards. Additionally, network information for both GSM and UMTS access can be stored, which improves the ability to offer dual-mode phones as wireless services evolve from 2G and 2.5G to 3G phones.

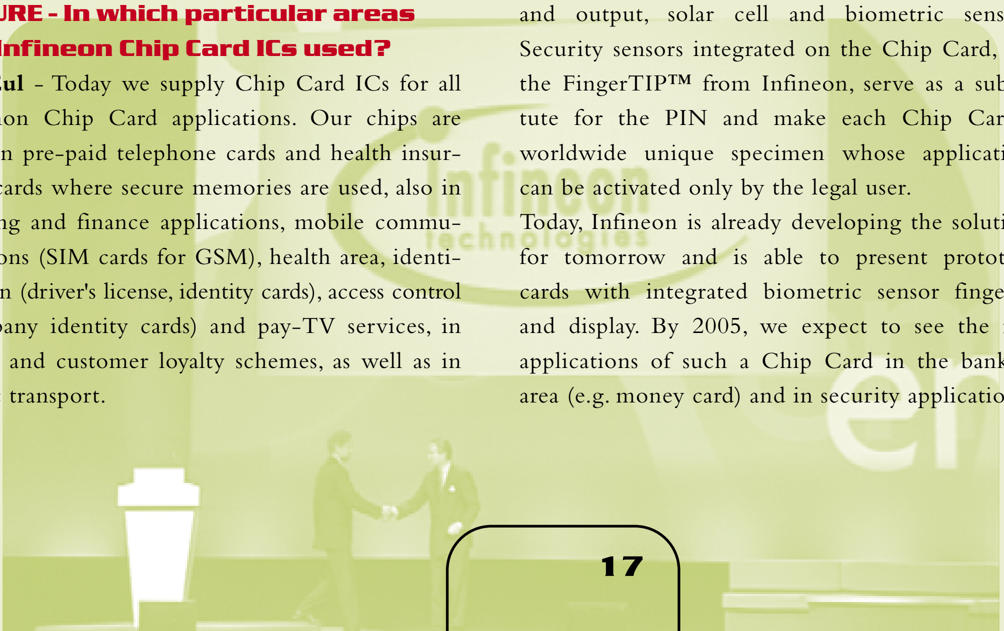
SECURE - What is the market situation for security and Chip Card ICs at the moment?

Dr. Eul – Like before, there is a solid growth in the area of "Banks & Finances" with bank and credit card applications. What is worth mentioning here is the bank project in Germany and the beginning of the changeover from magnet strip cards to Chip Card ICs by the large credit card companies. Infineon is one of the main suppliers for these applications.

The high growth rates of previous years, unexpected even for the industry, have not continued this year in the cellular phone market. In addition to this slowdown in growth, there is another reason that greatly affects the demand behavior: our customers are currently reducing their own stocks.

SECURE - In which particular areas are Infineon Chip Card ICs used?

Dr. Eul - Today we supply Chip Card ICs for all common Chip Card applications. Our chips are used in pre-paid telephone cards and health insurance cards where secure memories are used, also in banking and finance applications, mobile communications (SIM cards for GSM), health area, identification (driver's license, identity cards), access control (company identity cards) and pay-TV services, in bonus and customer loyalty schemes, as well as in public transport.

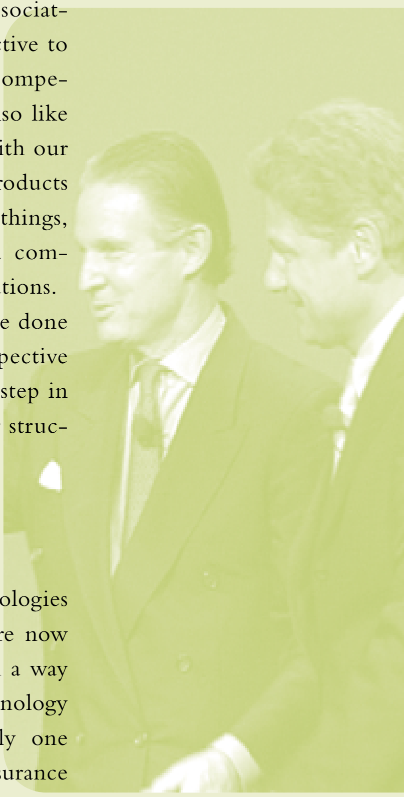


SECURE - What are your future objectives for the Security and Chip Card IC division at Infineon?

Dr. Eul - Ever since Infineon has entered the area of chips for card applications, it has acquired extensive expertise in the security aspects associated with this technology. It is our clear objective to retain Infineon's top position in this core competence area - even in the future. We would also like to use our security skills and couple them with our Chip Card ICs for other semiconductor products and applications. This includes among other things, one-chip security solutions for secure data communication and electronic commerce applications. For future Chip Card applications, as we have done in the past, we would like to provide the respective optimum Chip Card IC solutions. The next step in technology will be the jump to even smaller structural widths of 0.13 micrometer.

SECURE - How do you view the future of Chip Cards?

Dr. Eul - Progressive semiconductor technologies enable higher chip capacity. Therefore, we are now able to utilize Chip Card technology in such a way that was unimaginable at the time this technology was first introduced. Chip Cards with only one application, such as telephone or health insurance cards, will become multi-application cards. For example, these could combine the personal identity card with the bankcard, credit card, and the monthly pass for public transport systems and the customer card of a retail company on a single Chip Card.



Dr. Eul at the Europay Members Forum, Munich 2001

Moreover, the Chip Card, also known internally, as the chip-on-card, can be developed into a comprehensive system-on-card product - a highly secure computer in Chip Card format. Such a card will comprise of an effective Chip Card IC and numerous interfaces such as display, keyboard, voice input and output, solar cell and biometric sensors. Security sensors integrated on the Chip Card, like the FingerTIP™ from Infineon, serve as a substitute for the PIN and make each Chip Card a worldwide unique specimen whose applications can be activated only by the legal user.
Today, Infineon is already developing the solutions for tomorrow and is able to present prototype cards with integrated biometric sensor fingertip and display. By 2005, we expect to see the first applications of such a Chip Card in the banking area (e.g. money card) and in security applications.

Infineon Number 1 for Third Time

Gartner Dataquest has named Infineon Technologies the leader in worldwide sales revenue for silicon chips used in Chip Card products, marking the third consecutive year that the company has ranked Infineon as the number one provider of silicon to this fast growing market.

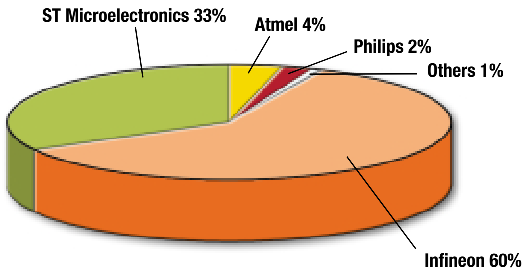
In its recently published report, the market research firm states that Infineon held a 47 percent share of the total 1.9 billion Chip Card IC market, representing 921 million units shipped.

In terms of revenue, Dataquest assessed Infineon's year 2000 shipments of both Smart Card microcontrollers and memory chips at 34 percent of the total market of approximately 1.2 billion US dollars. In 1999, Dataquest reported Infineon as holding the number one position with an overall revenue market share of 43 percent and, in 1998, revenue market share of 42 percent.

“Due to semiconductor supply restrictions within a strong growth market, Infineon and other major suppliers in previous years did cede some market share to new players,” said Andrew Phillips, Chip Card industry analyst within Gartner Dataquest's semiconductor group and author of the report “Worldwide Chip Card Market Share, 2000: Card Vendors and Semiconductor Vendors”.

Worldwide MEM Chip Card IC Market 2000 acc. to Dataquest Total Market in Mio. Pieces

"...Infineon Technologies dominated the supply of silicon to the memory card market with 60% market share...“ *Andrew Philips, Dataquest*

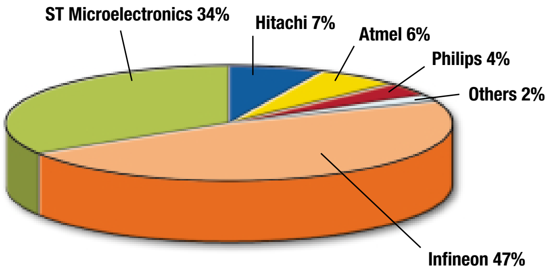


Mio. pcs.; Market Memories: 1,179 Mio. pcs.

“Infineon is pleased that its worldwide ICs leadership for Chip Card applications has been confirmed for the third consecutive year,” said Hermann Eul, Senior Vice President and General Manager of Infineon's Security and Chip Card ICs business group. “We have been at the forefront of security development for many years, and this expertise is a strong contributor to our leadership role. We are committed to maintaining our position in this core competence area.”

Worldwide Chip Card IC Market 2000 according to Dataquest Total Market in Mio. Pieces

"...Infineon Technologies retained its position as the major supplier of silicon for chip cards ...“ *Andrew Philips, Dataquest*



Mio. pcs.; Market in total: 1,942 Mio. pcs.

The Chip Card market is driven by the trend towards increased security requirements in such aspects of everyday life as mobile communications, banking, health services, electronic commerce and Internet communications, and government applications.

Infineon was the first supplier of Chip Card ICs to pass the strictest security evaluation tests for Chip Card ICs; achieving the ITSEC E4 high rating for multiple products.

According to Dataquest, Infineon dominated the supply of silicon to the memory Chip Card market with 60 percent market share in 2000. This is due to strong demand for security memory ICs for use in prepaid phone cards, especially in Asia and South America.

In the year 2000, Infineon was the first manufacturer to offer Chip Card controllers manufactured with state-of-the-art 0.25-micron process technology, which supported large on-chip EEPROM capacities of 64 kilobytes.

Bringing Biometrics and PKI together

By Magnus Pettersson, Product Manager, Precise Biometrics.

Introduction

To make biometric verification secure, it is important to store the biometric data in a secure way. To be able to keep the biometric information in a closed environment, it is essential that the matching be performed in the same environment as the data is stored.

This document describes the Match on Card technology, and why such technology is needed to gain secure biometric verification. The article also discusses Match on Card in combination with Smart Cards and PKI.

Biometric authentication

Biometric verification has the advantage of ensuring that only the correct physical user can gain access to certain information or areas. The biometric identity can never be borrowed, and it is up to the administrator of a system to decide who is to be granted access or not.

Enrolment and verification

During the enrolment (Figure 1), biometric data is captured. The data is processed, and a pattern is extracted. The pattern is chosen so as much unique information as possible is recorded. The extracted pattern is then stored as a biometric template.

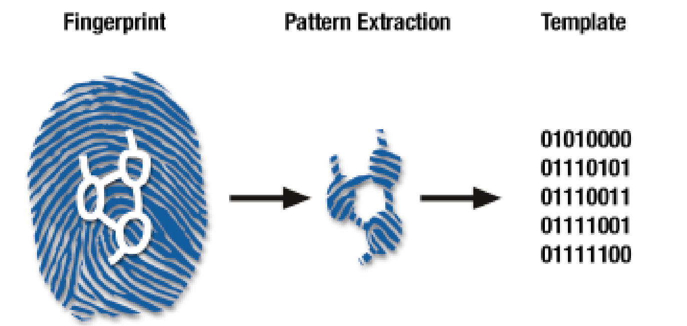


Figure 1 - Enrolment

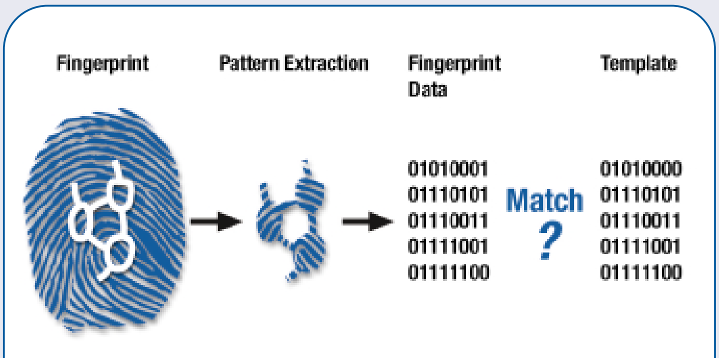


Figure 2 – Verification

During verification (Figure 2), a new pattern is extracted from the incoming fingerprint image. The pattern forms the fingerprint data that is matched against the stored template, containing the fingerprint information from the enrolment.

Why do we need Match on Card?

To gain maximum security, the biometric template must be stored securely in a closed environment. If the biometric matching procedure is performed outside this closed environment, it is exposed to the open environment, where anyone could steal the template. Even if the fingerprint template is protected by another security mechanism, this is to be viewed as the weakest link, and the biometrics does not really add any security.

The only way to ensure security, is to never let the biometric template leave the closed environment. In this case the biometric matching has to take place in this closed environment as well.

The Match On Card (MOC), technology solves this problem by performing the critical biometric matching in the closed environment, where the template is securely stored.

Match On Card

Match On Card takes its name from the implementation in Smart Cards. The match on card technology doesn't exclusively have to be used with Smart Cards as the secure device representing the closed environment. The same technology could also be used together with other secure devices, such as memory cards etc.

This article, however, is focused on the solution where the secure device is a Smart Card. The article also focuses on fingerprint verification, which is the kind of biometrics most commonly used.

The ideal solution for secure biometric verification would be that the fingerprint scanning and the matching were done in the same component. Today, no such device exists. Another ideal solution would be to send the original fingerprint image directly to the secure device, and that all processing was done there.

As the pre-processing is far too time consuming for today's Smart Cards, all operations cannot be done entirely inside this closed environment. The security can still be kept by dividing the process into pre-processing and matching and let the matching, where the stored template is needed, be done in the secure device.

The most important thing is that the stored template must never be exposed. Therefore only the part of the verification that requires the stored template has to be done inside the closed environment.

The process can then be described using the following steps:

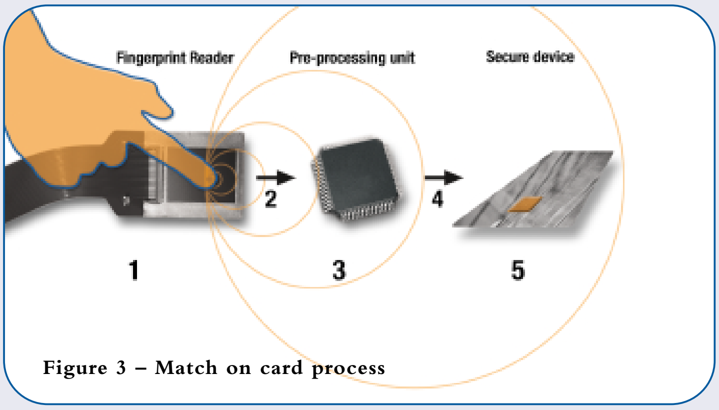


Figure 3 – Match on card process

1. The fingerprint image is read from the sensor
2. The fingerprint image is sent into the pre-processing unit.
   This pre-processing unit could be a PC or another device with enough capacity.
3. The fingerprint is pre-processed and the fingerprint data corresponding to the stored template is extracted.
4. The extracted fingerprint data is sent to the secure device (Smart Card).
5. The secure device matches the extracted fingerprint data against the stored template.

PKI

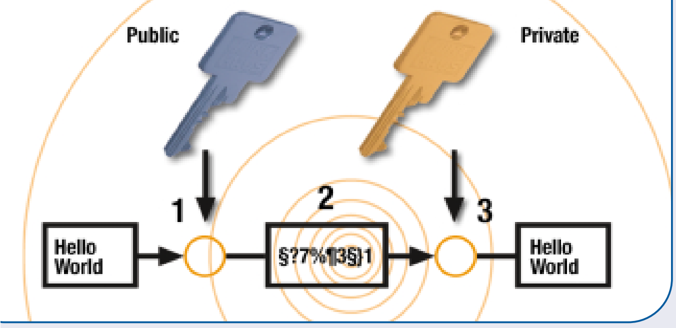
PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

Confidentiality	to keep information private
Integrity	to prove that information has not been manipulated
Authentication	to prove the identity of an individual or application
Non-repudiation	to ensure that information cannot be disowned.

PKI – How does it work?

The principle of PKI is built on the key pair. When a new key pair is generated, it will result in one public and one private key. Both keys are needed to encrypt and decrypt a message. If the message is encrypted with the public key, the private key is used to decrypt, and vice versa. Figure 4 shows how (1) the message is encrypted using the receiver's public key. (2) The message is sent encrypted over the net. The receiver decrypts the message (3) using his private key.

Figure 4 - Encryption and decryption using a key pair.



Normally the entire message is not encrypted using the key pair (asymmetric encryption), as it would be a very time consuming operation. Instead a symmetric key is generated for each session and sent to the receiver using his public key. When creating digital signatures the private key belonging to the sender is used for encryption. The public key of the sender can then verify the signature.

In Figure 5, this signature procedure is described. The information that is to be signed passes a known hash function (1), which compresses the data to a fixed size. The hash cannot be used to reproduce the original document. The hash is encrypted (2) using the private key of the sender (User A). The result of this encryption is the signature, which is placed together with the information in the message (3).

When the receiver (User B) wants to verify the signature, the message is hashed using the same hash function that the sender used (4). The signature is decrypted using the public key of the sender (5). The decryption of the signature using the public key of the sender should then result in the same data as the original hash. If the hash and the decrypted signature matches (6) The signature is considered to be valid.

The Public Key Infrastructure

A digital certificate contains digital information about the user, such as name, company, e-mail address etc. To create trust we need someone to guarantee the validity of the certificates. Therefore the Certification Authority (CA) signs all digital certificates. The issuer of the certificates, the Registration Authority (RA), can sometimes be the same instance as the CA, but in large infrastructures they are usually different instances. A comparison can easily be made with the physical world, such as issuing passports, ID cards etc.
Besides being the issuer of digital certificates the CA is responsible for the revocation of expired or stolen certificates. The CA also establishes registers of public keys for the certificates issued.

The Private Key

As the private key represent the identity of a person, it is very important that the key is stored in a secure way. Today the Smart Card is considered to be the best choice for secure storage of confidential information. As the crypto processor on the Smart Card itself performs the encryption using the private key, the private key is never exposed outside the Smart Card. Some cards today also have the possibility of generating the keys onboard the chip, which means that the private key is never visible.

However, the cards must be protected in a way that a stolen or borrowed card cannot be used by anyone else but the cardholder. The traditional way of protecting Smart Cards is by using a PIN. Still a PIN can be hard to remember, and they are sometimes written down. The PIN also has the disadvantage that it can be borrowed.

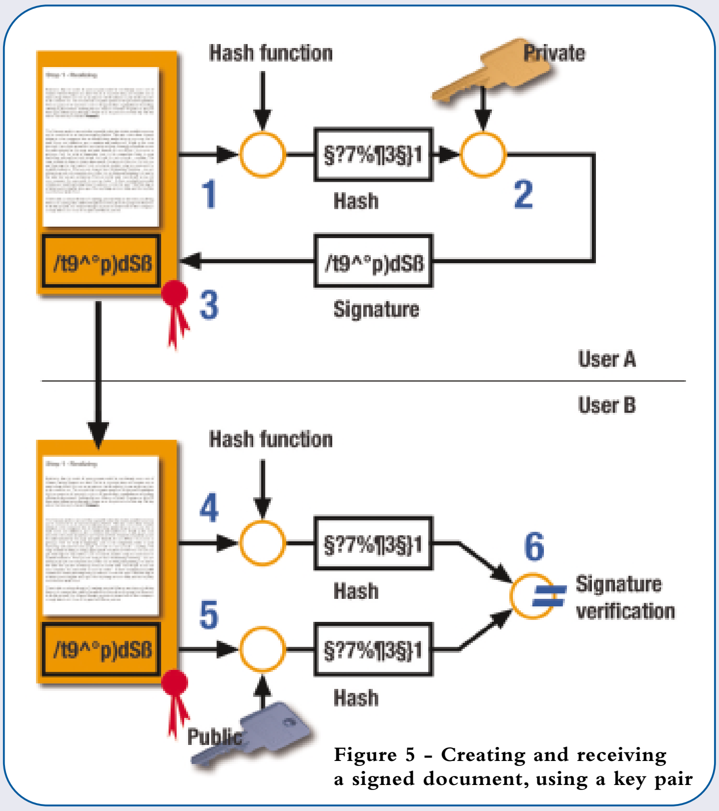


Figure 5 - Creating and receiving a signed document, using a key pair

The solution to the authentication problem is using biometrics, which cannot be borrowed or stolen. By using biometrics, we will achieve person-to-person communication instead of PIN-to-PIN communication, even in the digital world.

Biometrics, PKI and Smart Cards

The only way of securing a Smart Card with biometrics is to let the match take place in the Smart Card itself, where the biometric template is stored. If the match is performed outside the Smart Card there has to be some message sent to the card to unlock it. That message has to be created outside the card, and then the biometrics really doesn't add any security.

With Match On Card technology the Smart Card can be protected securely with biometrics. The match takes place in the secure environment of the card, where the template is also stored. The card will refuse to admit usage, if the biometrics does not match.

With Match On Card, biometrics will play an important role in making digital certificates personal. The following conclusions can be made.

1. PKI ensures security and trust in transactions, where the private key is the weakest point.
2. Smart Cards take care of the storage of the private key, where authentication to the Smart Card is the weakest point.
3. Biometrics ensures secure authentication to the Smart Card.

Conclusion

Match On card is a technology that makes the biometric matching inside a secure device where the biometric template is stored. The biometric template will then never be exposed outside the secure environment.

Together with PKI and Smart Cards, biometrics plays an important role in making the digital certificates personal, by refusing access to the private key without biometric authentication.

For more information visit:
www.rsa.com
www.baltimore.com
www.verisign.com
www.precisebiometrics.com

Secure Mobile Commerce

2000 was a landmark year in German mobile communications. The number of mobile subscribers doubled, rising from approx. 23 million in January to almost 50 million by year-end. This increase clearly paves the way for the widespread introduction of new mobile services [1]. The upsurge in numbers was fuelled primarily by a sharp increase in the availability of prepaid offerings. Mobile providers often subsidized the phone as part of these prepaid schemes, resulting in dramatic price reductions. The objective is to attract customers and promote long-term loyalty through subscription contracts.

Secure Mobile Commerce

Dr. Peter Laackmann
Infineon Technologies AG

The large-scale penetration of mobile devices has, for the first time, enabled the nationwide development of new mobility-enhancing services, centered in particular on mobile Internet access and a wide variety of m-commerce solutions.

Secure Authentication

All predictions for the evolution of m-commerce services over the next five years hinge on one critical precondition. The security solutions built into the systems on offer must ensure smooth electronic payment and reliable identification of trading partners. End-to-end security concepts for m-commerce systems are still in the early stages. The complexity of these security infrastructures is perhaps best exemplified through a comparison with "standard" electronic financial transactions (e-commerce, homebanking etc.). Encryption technologies can be deployed to protect the communication (telephone) lines against tapping. The PC terminal remains at the core of the transaction, however, and remains susceptible to attacks from programs such as viruses.

Two complementary approaches are available to protect against attacks of this nature. On the one hand, the customer must identify him/herself vis-à-vis the bank or merchant to ensure that the customer is actually authorized to order goods or execute a financial transaction (such as a bank transfer). The customer, on the other hand, has a vested interest in verifying the identity of the merchant to ensure that they are dealing with an authentic trader. The big danger here presents itself in the form of companies that set up fraudulent Web sites and disappear once they have received the cash without actually delivering the service or product. Sophisticated chip-card-based PKI (public key infrastructure) solutions already deliver robust protection against hoaxes such as this. Through the Chip Card, the trader/bank and customer exchange keys and authentication data. The card thus gives the customer a high degree of security. Building on this, a Trust Center is a neutral, third party instance that can easily verify the identity of the customer and the merchant.

The microcontrollers built into the Chip Cards must satisfy the most demanding security requirements to deliver reliable identification functionality.

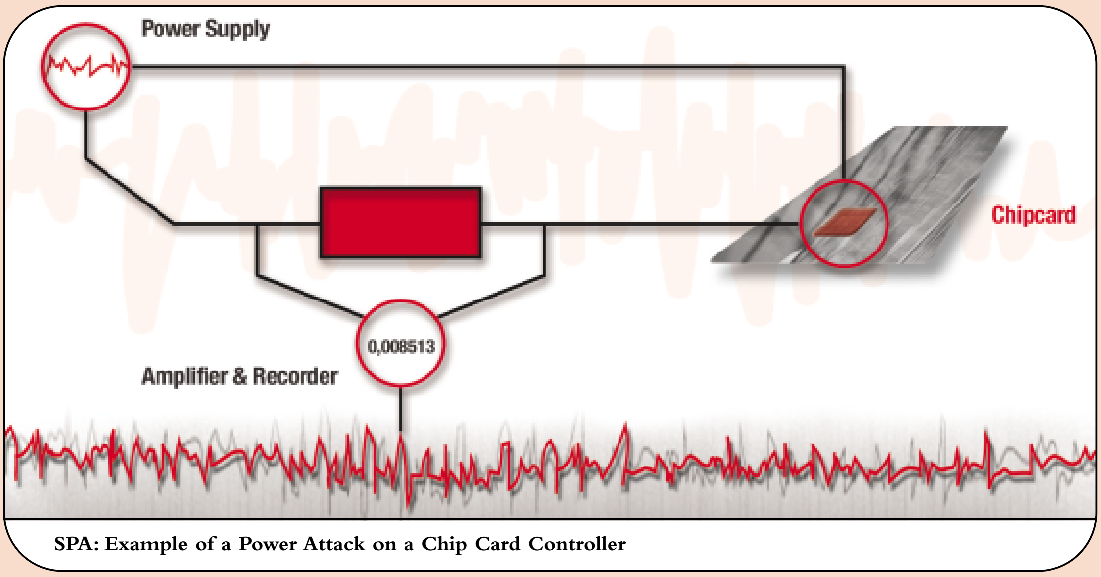
Moving from E-commerce to M-commerce

The inherently insecure design of a PC makes it a highly attractive target for hackers. The CPU cannot distinguish between legitimate and malicious software (i.e. user applications and virus programs). Thousands of viruses, Trojan Horses or espionage programs (such as key loggers, which record the keys hit by a user) have been identified. A group of leading players in the industry recently got together to launch an initiative aimed at enabling the customer and e-merchant/bank to check the security status of a PC before executing a transaction. The objective is to prevent malicious programs (such as viruses) from infiltrating the customer's transaction platform (the PC) and possibly manipulating the payment transaction. The TCPA (Trusted Computer Platform Alliance) has developed a security module known as TPM (Trusted Platform Module), which is integrated on the PC mainboard [2]. A TPM is also able to detect changes to the operating system software and individual program components (of homebanking programs, for example) and raise an alarm before the user enters into a risky transaction. TPM also monitors the booting process by means of hash functions, which generate a check value for large data volumes. In addition, TPM modules feature the most important PKI computing functions, such as the RSA authentication and encryption system. In short, TPM is a "trusted device". The TPM hardware significantly enhances the feasibility and security of a PC platform, particularly for e-commerce applications.

The prerequisites for a robust m-commerce security concept are similar. It must be feasible to reliably identify the customer, the merchant and the terminal; to securely exchange data and to protect the platform (the mobile phone) against a software attack. Hackers' successful attempts to crack SIMLOCKs provide clear evidence of the fact that software attacks are already commonplace in the mobile communications space. SIMLOCKs are protective mechanisms in the mobile phone operating software designed to restrict the SIM cards certified for any given phone. The ex-works settings can be modified on some mobile phones either from the PC (using an adapter cable) or on the device by checking certain values, calculating the release code and then entering the code manually. In future, mobile phones will require tamper-proof protection mechanisms.

Cryptography in Mobile Telephones

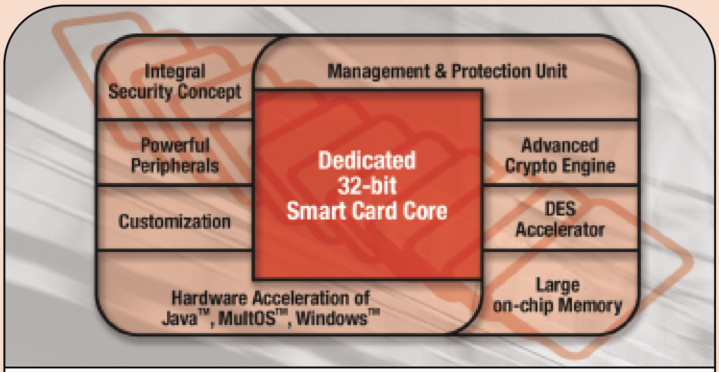
Nowadays, GSM mobile telephones are fitted as standard with a SIM (Subscriber Identity Module) card. The SIM microcontroller is used for identification – it authenticates the device when logging onto the mobile network and calculates an individual voice



SPA: Example of a Power Attack on a Chip Card Controller

encryption code for each call, which it hands over to the mobile phone [3]. This code is usually generated solely through a software mechanism stored in the ROM on the SIM card. For m-commerce transactions, the SIM card can act as a secure microcontroller, offering additional authentication and data encryption functionality. As the SIM card is supplied by the mobile service provider, however, the user has no guarantee that all necessary security applications can or have been integrated in the card. Mobile phones with additional card slots (dual-slot phones) or phones with a MultiMediaCard™ slot (such as the Siemens SL-45 described in more detail in the following), are thus interesting alternatives to single multi-function SIM cards. Another way to achieve the desired level of security functionality would be to install a hardware security module on the PCB. All of these approaches call for secure microcontrollers that are protected against attacks and manipulation.

Given that complete PKI solutions are required in addition to these relatively simple cryptographic calculations, tomorrows secure microcontrollers for m-commerce applications will require cryptographic hardware. Infineon's secure microcontrollers with a crypto engine feature; for example, a special long number calculator tailored specifically to the needs of modern PKI applications. This engine is optimized to handle fast computational operations with extremely large figures and is part of the integral security concept of the controller. As the value of transactions will rise over time, a secure microcontroller is obviously an attractive target for digital criminals. All of Infineon's next-generation controllers feature advanced mechanisms to counteract this. These include sensors, which monitor the precise operating conditions (such as voltage and clock supply) and various other ambient influences. They also feature mechanisms to protect against power analysis attacks (such as SPA - simple power analysis [4] and DPA - differential power analysis [5, 6]). These attacks have been carefully researched and much publicized over the last few years. Insecure microcontrollers are at significant risk of attack as they leak secret information on codes or classified transaction data to their environment over side channels. Measuring the power consumption of a microcontroller over time by means of a fast A/D converter and then analyzing these patterns with a computer is one such way of carrying out an attack. At a given time, critical information can be directly gleaned from the power consumption with SPA. DPA, on the other hand, requires statistical processes and is engineered to enable advanced analysis functionality for cryptographic processes such as DES or Triple-DES [7, 8].


Integral Security Concept
Management & Protection Unit
Powerful Peripherals
Dedicated 32-bit Smart Card Core
Advanced Crypto Engine
Customization
DES Accelerator
Hardware Acceleration of Java™, MultOS™, Windows™
Large on-chip Memory

Infineon's Secure Microcontroller from the 88 Family: Ideal Multi-application Platform for Future Mobile Cards

Highly effective Fourier transformation techniques are now deployed to protect against SPA and DPA. These measure even the slightest changes in power consumption and ensure a high degree of noise suppression. [9].

Protection Against Attacks

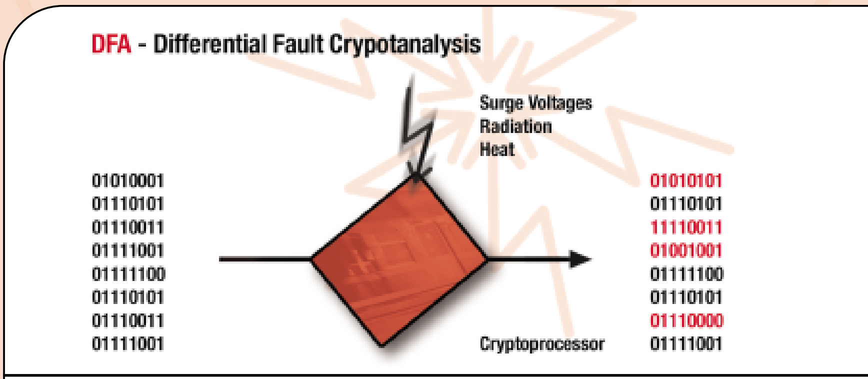
The features built into Infineon's secure microcontrollers specifically to counteract this type of attack ensure a high degree of protection. The very generation of information, which might be of interest to the attacker, is suppressed by means of a highly sophisticated architecture in the security-critical areas of the microcontroller. Infineon's secure controllers also offer optimum protection against tampering, which might involve, for example, placing ultra-thin metal needles on the chip surface and then probing and forcing signals [10, 11, 12]. A highly secure design coupled with active protective elements ensures a robust barrier against manipulation attempts. Secure microcontrollers are subjected to rigorous testing prior to certification. A microchip such as this must reach a specific security level in order to be certified for electronic payment.

Security standards are constantly rising to keep pace with rapid advances in attack technologies enabled through the availability of increasingly powerful devices. When developing secure microcontrollers, Infineon investigates and evaluates the possible tampering strategies we may be confronted with in the future, building appropriate countermeasures into the microcontroller design. The controller operating software must also comply with specific security requirements in order to be certified for use in connection with electronic payments. External interruptions to the program (caused, for example, by temporary power outages) must not result in errored calculations or otherwise expose the transaction to risk of attack. Attacks such as these are referred to as differential fault attacks (DFAs) [13]. These include manipulation of the power supply, temperature increases and exposure to radiation [14].

A secure microcontroller must also offer solid protection against forced faults such as these. To enable the necessary level of protection, countermeasures are deployed not only on the hardware side, but also through a range of software tricks, which detect errors, check data and computational results and help ensure fault-free operation of the microcontroller. Hardware and software security must be combined for optimal results. Only then can integral Chip Card security be achieved and this is precisely – in combination with cryptographic processes – what makes e-commerce and m-commerce solutions viable.

True Random Numbers

One of the key sources of cryptographic security is the random numbers generated in the secure microcontroller. These provide the foundation for secure, mutual identification and code generation. Pseudo Random Number Generators (P-RNGs) generate numbers by mathematically post-processing deterministic signals on the chip. The main disadvantage of P-RNGs is that the numbers generated must comply with certain mathematical rules and are thus predictable. To overcome this, Infineon deploys True Random Number Generators (T-RNGs) [15] in its secure microcontrollers. T-RNGs use a physical noise source, the output values of which cannot be predicted. Combined with public key crypto processes, this module enables reciprocal authentication between the card and terminal, and, working with the high-performance crypto engines, is also able to generate code pairs from the true random numbers directly on the card within a very short time period. This offers an advanced level of data protection as the secret code is generated directly on the customer side (and is thus not known to the card manufacturer or personalizer). This feature is of particular interest when authentication functionality is extended through the use of biometric technology. Mobile phones with an integrated fingerprint sensor (FingerTIP) have already been tested. The huge benefit of biometrics lies in the ability to physically verify the identity of the user. If a regular mobile phone falls into a third-party's hands along with the PIN, the third party can currently enjoy unrestricted use of the phone. If, however, biometric data is checked while the phone is in use, only the authorized subscriber can ever use the phone. If several subscribers have been authorized, the phone can distinguish between different access rights. Sensitive biometric data such as the digital fingerprint is also stored in and processed by a secure microcontroller.



DFA (Differential Fault Attack): External Interference Can Cause Errors in Unprotected Microcontrollers.

Just as biometrics-enabled and standard Chip Card systems currently co-exist in various applications for electronic payment and areas such as access control, the co-existence of various payment and financial transaction systems is expected in the mobile value-added service sector.

Siemens SL-45 with MultiMediaCard™

M-commerce and the MultiMediaCard™

Another new dimension was recently added to the mobile telephony landscape. The integration of a MultiMediaCard™ in the Siemens SL45 mobile phone enables data received through m-commerce transactions (such as an MP3 music file) to be stored directly on the phone's miniaturized, removable flash memory card and to be played or viewed on demand. Several megabytes of data can be stored on the MultiMediaCard™ (e.g. large telephone directories, maps, dictionaries etc.). The current card capacity of up to an impressive 64 MB already positions it as a data transport medium between terminals (such as digital cameras, portable digital assistants (PDAs), MP3 players, GPS navigation systems or even medical equipment) that use the MultiMediaCard™ as non-volatile memory. Thanks to the mobile phone interface, the user can read and edit data over the mobile network and the Internet.

Regardless of the application scenario, a secure microcontroller in the mobile phone presents interesting possibilities. It could be used to encrypt the data on the MultiMediaCard™, for example, thus protecting it against unauthorized access. The encryption code used for this would reside in the controller. The SL45 might even be compared with a PC: the same volatile memory, the hard disk is replaced with a non-volatile semiconductor memory; access can be protected by means of a secure microcontroller if required.

The MultiMediaCard™ can also act as a security element. A new hybrid solution currently being defined by the MultiMediaCard™ Association (MMCA), "Secure MultiMediaCard™", is of particular interest in this context. The Secure MultiMediaCard™ reveals far-reaching innovation potential on the application side. The application spectrum ranges from protecting copyrighted material (such as commercial music) against unlawful copying and privacy protection to attractive e-commerce and m-commerce solutions. One of the early signs of things to come in this area is the ability to download music, listen to it and pay for it from the mobile phone.

The last piece in the highly secure m-commerce infrastructure jigsaw is the mechanism to protect the actual phone itself. Similar to the TPM on the PC mainboard described above, a mobile phone can also be protected by means of a secure platform module, thus securing the operating software against direct attacks. The following looks at a particularly interesting end-to-end security concept deployed by the MeT Initiative.

MeT - Mobile electronic Transactions

Founded in April last year by the mobile communication specialists Ericsson, Motorola and Nokia, and since joined by Siemens, the MeT Initiative [16] aims to build the foundation for tomorrow's m-commerce solutions on the basis of a secure mobile platform, the PTD (personal trusted device). The MeT infrastructure defines three interfaces:

- Service Registration Interface handles customer registration
- Service Execution Interface executes the actual transaction
- User Interface ensures usability for the end user

The MeT concept provides for server (merchant/bank) and client (customer) authentication as well as for digital signatures and the encryption of data transmitted. The concept assumes that different modules divided into removable security elements and non-removable security elements will execute these functions. The former includes standard SIM/WIM cards or other removable cards with different form factors. A MultiMediaCard™ equipped with a secure controller opens up interesting new possibilities here. Founded in 1998, the MultiMediaCard Association MMCA [17] is currently defining a standard for a new MultiMediaCard™ with additional security, authentication and encryption functionality. Hardware modules, on the other hand, are non-removable. Similar to a TPM on a PC mainboard, they are integrated directly in the mobile phone chip. The same applies to software codes in the mobile phone operating system that enable the mobile terminal to be identified [18].

The functionality currently offered by mobile phones is set to evolve dramatically in the next few years, with data communication eclipsing voice telephony. Mobile financial transactions will emerge as one of the most important drivers of the new technology landscape. Secure microcontrollers and storage media from Infineon can turn our mobile devices into trustworthy instruments, making secure mobile financial transactions part and parcel of our daily lives. This secure technology could soon also become a standard feature of mobile telephony. Ultimately, end-to-end, integral security concepts are the key to ubiquitous mobile commerce.

References

[1] G. Singh, "Mobile Commerce: Erfolg durch Sicherheit [Success Through Security]", Card-Forum 24, 2000, 24-26.

[2] M. Scheibe, "TCPA Security: Trust your Platform", Secure - The Silicon Trust Quarterly Report 3, 2000, 44-46; general information on TPM and TCPA at **www.trustedpc.org.**

[3] M. Janke, P. Laackmann, "GSM: Schwachstellen in der Verschlüsselung [Encryption Weaknesses]", Card-Forum 7, **1998,** 44-47;J. M. Balston, "The Pan-European System: GSM", in J.M. Blaston, R.C.V. Macario, "Cellular Radio Systems", Artech House, Boston **1993**

[4] R. Mayer-Sommer, "Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards", in C. K. Koc, "Proceedings CHES **2000,** Workshop on Cryptographic Hardware and Embedded Systems, 17.08.-18.08.2000", Worchester, USA **2000.**

[5] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis and Related Attacks", Cryptographic Research, Inc., San Francisco.

[6] P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", Cryptographic Research, Inc., San Francisco **1998.**

[7] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards", USENIX Workshop on Smartcard Technology, Chicago, **10.05.-11.05.1999.**

[8] T. S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software", in C. K. Koc, "Proceedings CHES 2000, Workshop on Cryptographic Hardware and Embedded Systems, 17.08.-18.08.2000", Worchester, USA **2000.**

[9] D. Naccache, F. Olivier, "Blind Deconvolution and DPA Resynchronization", Presentation "CHES 2000, Workshop on Cryptographic Hardware and Embedded Systems, 17.08.-18.08.2000", Worchester, USA **2000.**

[10] R. Anderson, M. G. Kuhn, "Tamper Resistance - A Cautionary Note", University of Cambridge, Universität Erlangen, **1998.**

[11] M. Janke, P. Laackmann, "Simulation und Reverse Engineering im Chipkartenbereich - Neue Herausforderungen für Entwickler und Hersteller[Simulation and Reverse Engineering in Chip Card Technology – New Challenges for Developers and Manufacturers], Dokumentation Rednermanuskripte, International Exhibition and Conference for Card Applications, Systems and Technology, Wiesbaden 26.11.-28.11.1998", A la Card Verlag, Ratzeburg **1998.**

[12] P. Laackmann, M. Janke, "Chip Card Simulation and Reverse Engineering", A la Card Euro-News 10, **1999,** 103-105.

[13] Bell Communications Research, "Smart Cards Can Leak Secrets", Bellcore Press Release, Morristown, USA **5.9.1996;** Bell Communications Research, "New Threat Model Breaks Crypto Codes", Bellcore Press Release Morristown, USA **25.9.1996.**

[14] M. Janke, P. Laackmann "Wie sicher sind moderne Kryptoprozessoren ?[How Reliable are Modern Cryptographic Processors?]", Card-Forum 2, 1997, 53-54.

[15] P. Laackmann, "Mit Sicherheit gute Karten - Transparente Kryptographie: Neue Herausforderungen für Chipkarten-Entwickler [Transparent Cryptography: New Challenges for Chip Card Developers]", Elektronik 23, **2000,** 78-80.

[16] http://www.mobiletransaction.org/

[17] http://www.mmca.org/

[18] The MeT Initiative, "MeT Overview White Paper Version 1.0 - The MeT Initiative - Enabling Mobile e-commerce", 2.10.2000.

For many years PKI has been seen as the next logical step in IT to provide a new level of application security. But, PKI has still not really taken off yet and to date the promise that everyone would benefit from digital signing has not been fulfilled. However new players (at least in PKI time-scales) are now entering the game...

By Harry Knechtel & Omar Rifaat, © 2001 Secartis AG

PKI GOES Mobile

Asymmetric encryption as the basis for secure transactions

Asymmetric encryption, such as RSA or elliptic curve algorithms, is today well established as the basis for digital signatures. They are commonly used in different standards like SSL or S/MIME to secure different kinds of electronic transactions and enable data-integrity, strong authentication and non-repudiation.

The IT infrastructure needed to administer, publish and revoke the certificates that contain the essential data that securely identifies individuals – normally encapsulated in X.509 certificates – is known as PKI (Public Key Infrastructure). Such an infrastructure may contain one or more Registration Authorities (RA), Certification Authorities (CA), Directories (LDAP, OCSP) as well as the applications that make use of that infrastructure, and which in the end justify the existence of the overall system. Examples of such applications include transactional applications like restaurant bill payment or share dealing, as well as other forms of 'high value' applications like secure email.

Today intelligent Chip Cards – also referred to as Smart Cards- are recognized as a secure storage place for a user's highly confidential private key data. The ubiquitous SIM card that is a standard feature of all GSM phones is particularly well suited for private use by consumers, where hardware security modules (HSM) are either too expensive or inconvenient.

Mobile PKI

But now, with the WAP 1.2 specification moving forward, more and more mobile operators are entering the PKI scene. Also, since a complete mPKI is not specified by the current standards and protocols available on the market, it is clear that mobile network operators will not deploy a WAP-based mPKI until at least early next year. Some operators are enhancing their existing SIM toolkit infrastructure to enable PKI functionality, without having to wait until the long-promised WAP standards and hardware become available. (Particularly the Smart Card based Wireless Identification Modules -WIM and SWIM). Such operators, which include Vodafone, are seeking to take the early-mover advantage and be the first to offer secure value-added applications to their customers.

Taking the Vodafone implementation as an example, the overall process required to implement an SMS-based mPKI solution is described in Figure 1.

At this point the user is able to use digital signatures. The signing process itself has five basic Steps, as seen in Figure 2.

Optional to this scenario, the verification system could also be located at the application service

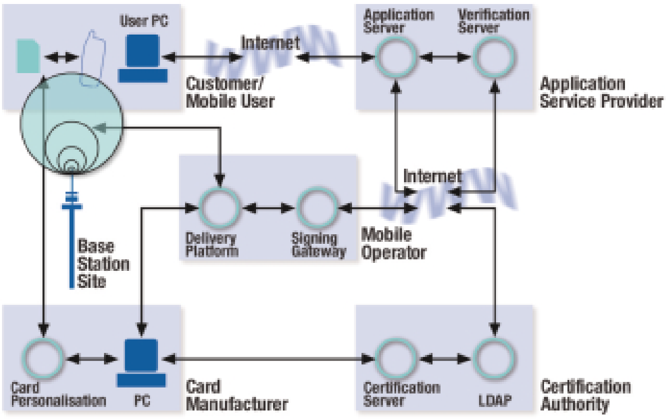


Figure 1.

1. The card manufacturer creates PKI enabled SIM cards. In addition to the normal process, public and private key pairs have to be generated.

2. The private key is securely stored away on the SIM card and the public key has to be forwarded to the Certification Authority.

3. The SIMs are distributed to the customers.

4. When the customer finally applies for digital signature, a registration process is started and a notification is sent to the CA, to create a certificate from the pre-stored public key associated with the user's SIM.

5. The new certificate is published through the directory of the Certification Authority.

6. In order to complete the registration, the signing functionality on the SIM is unblocked and a signing PIN (S-PIN) is assigned to the customer.

provider (ASP), who would then directly access the certification authorities directory, either through the lightweight directory protocol (LDAP) or the online certificate status request (OCSP).

The mobile infrastructure solves traditional PKI problems

One major advance for the mobile operator is that he has already a lot of the infrastructure needed in place. The problem of issuing and distributing SIM cards is quite common to mobile operators. Also they already have a network for support and revocation in place that can be used for the new task. Another benefit here, is that the customer is already used to receiving Smart Cards from this kind of supplier, so it is quite natural for him to be provided with this technology by the operator. Another technical advance for the operator is that he is always in control of the signing device. So if a SIM got stolen or lost, revocation could not only be established by putting a certificate on a revocation list (CRL), but the signing device itself can be disabled on the fly over the air (OTA).

The mobile handset is the VW Beetle of card readers

But still the major benefit seems to be that the penetration of mobile phones within society – especially for the targeted customer base - is quite big. And within the mPKI there are no distribution problems for card readers and Smart Cards – one of the major cost factors within traditional PKIs – as everyone already has one. So the mobile phone is really the low-cost card reader solution for the mass market.

mPKI solutions are already in place

One example for a successful mPKI build on SMS technology is the Vodafone DTI trial, which was started this year. Within this project Vodafone UK provided a platform and application for the UK Government, i.e. the Department of Trade & Industry (DTI), in order to enable them to digitally sign expense claims – created on a WEB interface - using the mobile phone. Employees of the DTI no longer have to work through piles of papers in order to fill out their claims and get their expenses paid; they simply log onto a web site and put in their data, whenever and wherever they want. Finally a receipt is created and sent to the mobile phone in order to be signed. The system is even powerful enough to support the whole process flow from claiming the expenses through authorization, to obtain final acknowledgement for the transaction.

In the case of Vodafone, several partners worked together to build the infrastructure: Vodafone UK provided the network and, as major stakeholder, led the project; GlobalSign provided the needed Root and CA certificates; Giesecke and Devrient (G&D) provided the mPKI enabled SIM cards; SmartTrust delivered the needed security and gateway technology; while Secartis took the leading role as overall system architect and guided the specification and construction of the system. In order to speed up rollout of the pilot, Secartis generated the public key certificates for the SIMs using its pre-existing interface with the G&D card production facility.

New tasks and opportunities are generated by mPKI

Judging by the success of the Vodafone implementation, there is a bright future for mPKI. Together with new developments in sight on the legal front, digital signatures are gaining legal acceptance. On the technical side, WAP 1.2, WIM and SWIM are moving steadily ahead. In summary, we at Secartis, expect that mPKI will soon provide the basic infrastructure upon which a whole new generation of m-Commerce applications will be built — including many applications, which have not even been thought of yet!

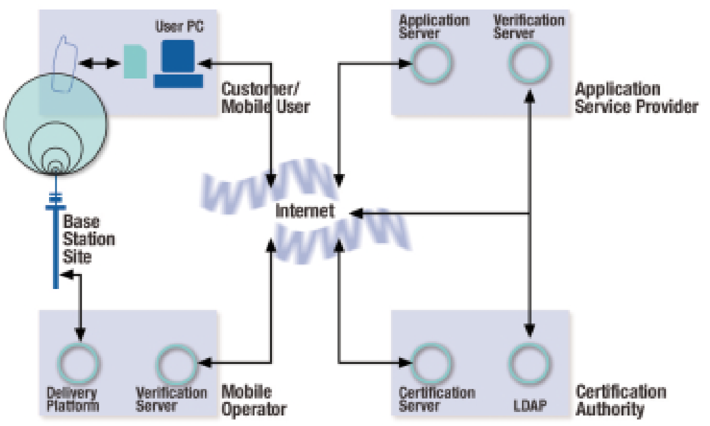


Figure 2.

1. The application sends a request to sign certain data to the security gateway at the operator.

2. The request is converted into executable SMS bytecode that can be interpreted by a plug-in on the handset and is sent to the user.

3. The user gets a request on his handset and now must enter his S-PIN in order to allow the phone to digitally sign the incoming data.

4. The signed data is returned to the verification system at the operator. This requests the matching public key certificate of the SIM that should have signed the data and uses it to verify the signature.

5. Finally, a response is created whether the signing was successful or not and is returned to the application server.

Putting their Cards on the Table

An Interview with Giesecke&Devrient

From banknotes to Biometrics, G&D have always been at the forefront of payment, telecommunication and security products. With new security challenges arising in the market, SECURE spoke to John Atkinson, V.P. Strategic International Marketing at Giesecke & Devrient about his thoughts on USB Token security versus Smart Card security, the latest Biometric developments at G&D and why G&D joined a Security Platform called the SiliconTrust.

>>> There is a trend towards increased security requirements in such aspects of everyday life as telecommunications, banking, electronic commerce and Internet communications, which call for new security solutions. Where do you see the key advantages of the USB Interface for Security Applications?

John Atkinson – Concerning security applications the form factor does not influence the security of applications very much. The high security is given by the secure micro controller (hardware) and the secure design of the operating system software. As G&D we have had our STARCOS® SPK 2.3 operating system ITSEC E4 high evaluated – in compliance with the German and Austrian Signature Law –, with a well defined and high level set of security targets. We are currently undertaking FIPS compliance testing and will also undergo Common Criteria testing, thus ensuring a global certification.

One can "add" hardware security by introducing a sophisticated housing to the token. But the best security concept is always to combine software and hardware security for most efficiency.

We adhere to all Smart Card standards like ISO 7816 or ISO 14443.
One key advantage of the USB Interface is standardization. Supported by a consortium of manufacturers, currently more than 400 million PCs carry a USB port. USB allows for easy plug-and-play connectivity and high transmission rates. In the case of tokens, card readers are not necessary and the USB Interface does not need an extra power supply.

>>> Do you expect the USB Standard to replace ISO as the standard of modern information and communication equipment? If so, what effects do you think this will have?

John Atkinson – We do not believe that USB standards will replace ISO standards. ISO standards define much more than just the communication between devices and a PC. USB is a very convenient option for connecting a reader, a token, a handheld or any other devices with a computer.

As we are in a dynamic market, even though it is currently facing some challenges, we will clearly see significant changes in standards driven by market requirements. We expect USB to supplement the existing series of ISO standards. In some applications, certain layers of the ISO protocols might be replaced by USB.

>>> Will Giesecke & Devrient offer a Plug-and-Play USB Smart Card & USB Token in the near future?

John Atkinson – G&D currently offers a smart USB token based on the market proven G&D ITSEC E4 high evaluated STARCOS® SPK 2.3 operating system as a toolkit. A Smart Card with USB interface is not available yet. It would require a single-chip solution for the security chip and USB controller.

Due to cost considerations, we expect smart USB chips to be available within the next 6-12 months enabling true USB/SC token products to be offered to the market.

A "full" Plug-and-Play USB token can only be achieved if the middle ware and token software is embedded in the PC's operating system. With this approach you do not even need to deliver a CD with the token manufacturers software.

>>> The implementation of a Smart Card Infrastructure can be costly and time consuming. Which applications call for the form factor Token and which for the Smart Card?

John Atkinson – Basically, mobile PC applications call for the USB token, namely signature applications, PKI, Web-Access, VPN, home banking and of course logon and license control. Price-sensitive applications may open up for the technology, when more economic tokens are used instead of a Smart Card plus reader. This will create additional business and will

definitely not lead to cannibalization effects relative to Smart Cards.

However, the classical card applications like ATM cards, ID cards and others will, for several reasons, rely on the form factor Smart Card. The card is established as a payment and identity device and a wide infrastructure of readers is already deployed. Some applications require more printing surface than available on a convenient token. Automated large-scale completion and personalization for tokens are currently unresolved tasks. Another categorization is of a psychological nature: Banking cards are usually kept like cash in the wallet, whilst the key ring commonly comprises physical or electronic keys to unlock and access applications.

>>> With the USB developments, new companies are moving into the hardware security arena. Where do you see Giesecke & Devrient's Key Competencies and how do you differentiate from other players in the market?

John Atkinson - Giesecke & Devrient has a long history as a provider of security products to large government organizations (first bank notes printed in 1856) and therefore a privileged position as a trusted partner.

Driven by the explosive expansion of e-commerce, e-business and IT security, comprehensive solutions are increasingly gaining importance. The market potential is highly jeopardized without appropriate security technology. G&D has intensified its activities in the field of security; to this end we have set up our subsidiaries Secartis AG for network security and CpayS AG for secure electronic payment. G&D offers comprehensive consultancy services and individual, tailor-made solutions. G&D is constructing a global network of partners. The Silicon Trust platform is a consequent step in this direction.

>>> What are the latest developments on Biometrics at Giesecke & Devrient?

John Atkinson - We have implemented the on-card-matching technology in collaboration with a partner company. The biometric fingerprint verification on card is fully integrated in the operating system.

Continuous improvements on G&D´s match-on-card solution with smaller template sizes (reduction of more than 30 %), faster transmission rates (10 times faster), better matching performances and increased free application memory space (> 20 kb) will further enhance user acceptance in the emerging biometrics markets.

G&D is highly convinced about the match-on-card technology due to the fact that this solution provides highest security levels combined with utmost privacy. As the reference data will never leave the card, highest security levels are guaranteed. Particularly within high security applications (PKI-Infrastructure) biometrics will replace passwords and PINs to a larger extent in the near future. Integrating Smart Cards, biometrics and public key cryptography provides a solid foundation for developing secure applications and communications.

G&D will focus on fingerprint solutions considering the fingerprint technology as the oldest and most widely accepted one. In addition, fingerprint sensors offer presently the most economic solution – the cost factor is still one of the industry barriers for a widespread adoption of biometrics.

>>> As Chip Card technology advances, Infineon envisions many key developments. Today's chip-on-card products will likely evolve into a complete system-on-card or even a highly secure Chip Card-sized personal computer. This advanced product will likely include a powerful Chip Card IC, biometric sensors, flexible LCD display, keyboard, microphone and speaker, and solar cell. Giesecke & Devrient and Infineon Technologies are already working on next-generation solutions in this area. Please describe Giesecke & Devrient's activities to bring these new components to a Chip Card. Are there specific challenges? How did you master them? When do you think the technology will be mature enough for market introduction?

John Atkinson - G&D is committed to support any effort in this direction. Since some of the technologies required for such a card are not core competencies of the Smart Card manufacturer the developments are made in co-operation with technology partners, especially with regards to miniaturization of some key components in order to fit into the card or token form factor.

First prototypes with G&D display cards are already being tested for evaluation in some key markets. There is actually a big potential market of complete new applications. We are working heavily on a robust display technology and processes to incorporate the displays into the card body (card stock).

G&D believes in a complete system-on-card. The main challenge of course is the consideration of the ISO 7816 standard. Widespread rollouts of ISO conform "system-on-card" Smart Cards will still take some years. But we will take up the challenge!

>>> What do Giesecke & Devrient see as the main benefits for joining a security platform such as the Silicon Trust?

John Atkinson - The Silicon Trust partner program is a very professional managed industry platform, which will particularly help the biometric industry to pave their way in the future. Silicon Trust definitely supports G&D to communicate credible and effective security applications with the natural add-on biometrics. As mentioned, markets are asking for end-to-end solutions; Silicon Trust is bringing the right partners together. Particularly for our subsidiaries, local partnering with Silicon Trust members is a big chance.

The exchange of information amongst the partners will increase our market awareness.

As a technology forum, Silicon Trust can help any participants in collaborating closely with other professional companies on standardization and development of the next generation products.

SmartUSB The Integrated Solution for Personal IT Security

By Thomas Roeder, Infineon Technologies AG

Today, Smart Card products mainly provide personal IT-security. These Smart Cards give access to corporate IT-networks and support RSA-cryptography for digital signature purposes. Although Smart Cards are quite cheap, the final cost of ownership is much higher due to the fact that each PC and workstation need to have a Smart Card reader installed to communicate with the Smart Card. A readerless solution could significantly reduce the cost of ownership and at the same time drastically increase the market demand for such solutions.

USB-Tokens also known as USB-Dongles are one alternative. Another solution will be USB-Smart Cards. Both devices can be connected to a PC using the standard USB-interface, which is widely spread in all PCs installed in the field and implemented in every PC currently shipped. Thus the need to install an expensive Smart Card reader does not exist anymore. The USB-Dongles can be directly plugged into a PC's USB-port while an USB-Smart Card only needs a simple and cheap connector to be connected to USB.

Schlumberger announced the rollout of the first dual-interface USB/ISO-Smart Cards during the second half of 2001. USB-Dongles are in the field already. The market lift-off of this new form factor is currently taking place.

The success of both form factors – USB-Smart Card and USB-Dongle - mainly depends upon solving the problem of the integration of an USB-interface into a secure Chip Card controller. SmartUSB is Infineon's solution to this particular problem. SmartUSB will significantly reduce the bill of material for USB-Dongles. This is the basic prerequisite for the market success of USB-Dongles. But SmartUSB will also allow the simple integration of an USB-interface on a Smart Card.

SmartUSB - The Product

SmartUSB combines the security of Infineon's ITSEC E4 High certified SLE66CX640P Controller with the speed of USB. The integration of a USB-interface provides a powerful single chip solution for USB-Tokens such as Dongles and USB-Smart Cards.

Beside the USB-interface there is still the standard Smart Card ISO7816-interface available. The combination of both interfaces on one chip allows a simple integration of a Dual-Interface USB/ISO-Smart Card. Such a Smart Card will be fully compliant to ISO7816 on the one hand, while on the other; the USB-interface will provide easy and high speed-connectivity to the IT world. So the requirements of both current existing infrastructures – Smart Card and IT-infrastructure – can be satisfied using one single device.

SmartUSB also provides all relevant hardware accelerators for symmetrical and asymmetrical cryptography. The ACE (Advanced Crypto Engine) supports RSA cryptography for bit lengths up to 1024 bits. Bit lengths of 2048 bits can be supported using the Chinese Reminder Theorem. Beside this, the ACE architecture can also calculate elliptic curves (EC) cryptography according to GF(p). The DES engine provides DES and 3DES cryptography as well as EC cryptography according to GF(2n). A dedicated high-speed hashing accelerator supports SHA-1 and MD5 algorithms.

New applications

Today the main applications of Smart Cards and USB-Dongles are authentication or PKI applications. In these cases the secure controller is only used for secure key storage, digital signature and key exchange for symmetrical cryptography. All symmetrical cryptographic functions, where huge data packages with according data rates are generated, are implemented on the host platform. This is, of course, the only feasible solution today, due to the fact that the standard Smart Card ISO7816-interface does not offer sufficient data rates for bulk encryption/decryption.

The USB-interface might be able to change the current situation. Effective data rates of up to several Mbit/s are possible. Just as a comparison - that's the typical speed for widely spread Ethernet-implementations (10 Mbit/s). Another example: Many companies use E1/T1 lines with 2 Mbit/s to connect several company locations within a VPN. Typical home Internet access solutions provide data rates ranging from 56 kbps (analog modem) via 64 kbps (ISDN) up to 1-8Mbit/s (ADSL or SHDSL). Having a fast USB-interface does not necessarily mean that there are no other bottlenecks anymore that would limit the maximum data rates supported by an USB-security controller. However, through the use of the Infineon crypto-accelerators, these data rates can be supported as well. Symmetrical cryptography up to data rates of 1 Mbit/s is not a problem at all. Hashing accelerators are even faster. Using such devices, new applications beside PKI and finance applications could easily be provided to the end customer.

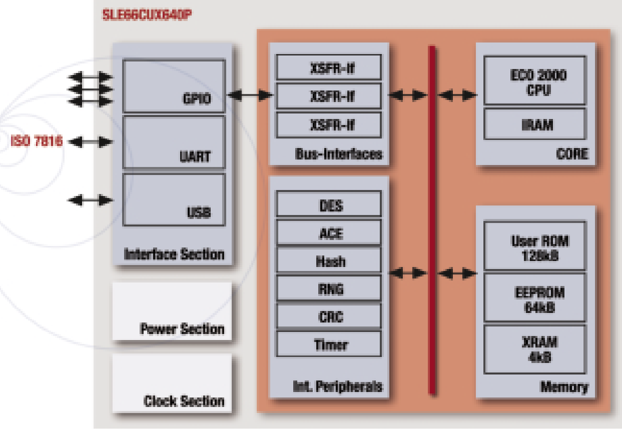


Figure 1- Architecture for the SmartUSB

Such applications could be:

- Highly Secure Digital Right Management Solutions.
- Fast, smart, portable and Secure Flash Memory Dongles with storage capacities of several 100 MByte, no bigger than a typical USB-Dongle today.
- Encryption/Decryption devices for teleworkers
- Complete Firewall solutions including encryption/decryption accelerators for home applications

The market potential is huge. The hardware costs using USB-Dongles are quite small considering the high security advantage brought about through such hardware solutions.

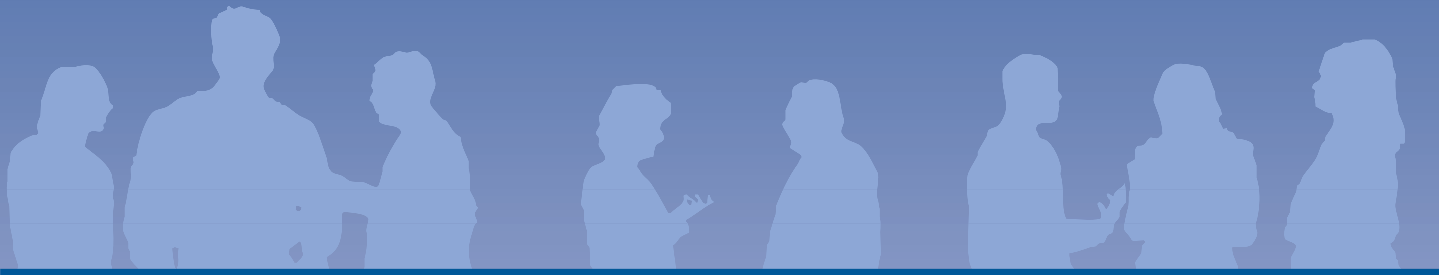
Let's take the example of a firewall on an USB-Token to give a better feeling of what's possible.

Let's assume that you use a PC based on a secure platform as defined within the TCPA-initiative (Trusted Computing Platform Alliances). The goal of this initiative is to provide a hardware or PC platform, which is able to verify the data integrity at least every time the platform is booted. Meaning that any contamination of the platform with viruses or any unauthorized changes of the platform can be easily detected. Infineon provides a device that is specified to TCPA standards and specifications, called the Trusted Platform Module, or simply TPM. Together with an efficient firewall solution based on SmartUSB, hackers and virus attacks from external networks and from contaminated data storage devices such as CDs can be blocked.

Sounds difficult - or even expensive? Not at all! SmartUSB as well as TPM are low cost devices, compared to current hardware solutions for IT-security. Additionally they provide a leading edge and field-proven security architecture. In fact, it's time to re-evaluate the target applications of security controllers. They're not just Chip Card controllers anymore. Their target applications range from simple authentication or access control, up to networking or communication applications and beyond. You could almost say that the Chip Card controller is finally growing up – it's definitely becoming smarter!

Securing the Information Society
A new European Union

By Barbara Frey, Faktum Softwareentwicklung



The "information society" and the benefits to be reaped from it for the next generation of citizens, is the focus of a project initiated by the European Commission. The declared goal of this EC project is to bring communities closer together, to create wealth and encourage the sharing of knowledge. By accelerating the technical development of convenient, user-friendly e-security media, which is focused on actual situations in the countries of the European Community, a huge potential exists which could enrich the lives of everyone. Within this innovative EC project, FAKTUM is playing a crucial role as the partner for the development of the software security components.

When it comes to e-commerce and e-finance in Europe, security is considered one of the most important elements. E-government and e-health could certainly benefit from a thorough review of their security. It is common knowledge that the majority of Internet users hesitate to take advantage of e-commerce offerings, due to doubts about the security of their transaction. With increased media attention highlighting successful attacks on upcoming transactional systems to the general public, confidence can easily falter, not only in the e-commerce sector, but also in the electronic payment infrastructure too. Therefore eliminating this prospective security leak is one of the most important tasks in supporting e-commerce and ensuring its future.

To accelerate positive changes in Europe, the European Commission has introduced different programs to support the European dimension of an "information society". These EU-programs are characterized as follows:

- The primary goals of the project and the user tests have to cover European interests and require common, progressive European solutions.
- The participants have to be from different European countries. Each country brings its individual ideas, to achieve a broad, useable solution.

Under these preconditions, the Smart USB consortium has been created to co-operate in these ambitious and innovative developments.

The goal is to make available an advanced, high level and user-friendly security product which can easily be used by every interested EU-citizen and which is not blocked or limited by foreign export regulations. The advantages for other IT programs initiated by the European Community, is that by using such a secure, comfortable, and cost effective security medium such as Smart USB, it has a role to play in a wider range of secure applications in the area of e-government, e-health, e-banking and m-commerce.

The partners within this consortium and their specific contribution to the project are:

- Infineon Technologies AG, Germany, (chip design and development)
- NewLogic Technologies AG, Austria, (chip design)
- Sphinx Electronic GmbH, Germany, (hardware design and development)
- Dresdner Bank AG, Germany, (real e-banking test environment)
- Asociation Centro Alto Technologia en Analisis Imagen (CATAI), Spain, (development and test of an e-health application)

FAKTUM as an IT security specialist supplies the necessary security software components as well as the e-banking solution.

The following shows the present technological situation: Smart Cards and cryptographic tokens are the hardware based security media for the "information society" in Europe. These main security mechanisms, together with a comfortable and secure storage capacity, allow the protection and support of most of the current information, communication and transaction structures.

But for comfortable activities, especially mobile ones, the usual Smart Cards are not always the optimal solution. Their use requires an appropriate card reader, which results in trying to offset the cost of this necessary hardware, especially in a low cost segment. The Smart Card reader is not easy to handle, may obstruct a required serial connector on the PC already used for other devices, or the necessary software drivers may cause problems – obstacles, which might de-motivate the average user not to use such an additional hardware component. This, consequently, leads to the fact that sometimes security might be neglected in favor of convenience.

But there are other technical means to ensure end-to-end security. Modern information and communication devices already have an easy to use USB connector with the necessary drivers and software support, which could be used for future oriented solutions. So the solution is to add a USB interface to an existing security Smart Card chip. This Smart USB token will enable and improve the comfortable e-commerce activities that net consumers deserve today.

Due to its definition as a user friendly, intelligent security medium, the new Smart USB token will offer a wide range of applications and functions:

- Integration of different homebanking standards and applications
- Different e-commerce standards and applications
- Implementation of further PKI applications
- Securing mail by storing keys only inside the module
- Encryption of PC files inside the module
- Access control, authentication and identification
- Authentication and identification: Storing securely personal biometrics reference data
- Multi applications - just one module can serve all major applications.

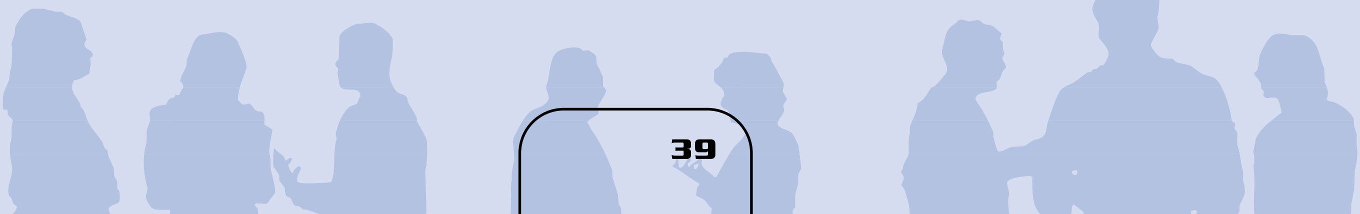
Based on these prerequisites, the next steps of the Smart USB consortium are to be the addition of a USB interface to an existing security Smart Card chip, the adaptation to a typical e-commerce and a health care application, the execution of a test with a major banking application, as well as execution of a test with a health care application. These tests will take place in two different European countries, Germany and Spain.

FAKTUM as an IT security specialist with competence in advanced Smart Card technologies and a wide knowledge in secure banking applications, is contributing important software development to this ambitious project. This includes the development of the CT-API adaptation layer for the improvement of existing Smart Card applications and the implementation of FAKTUM's HBCI application for Dresdner Bank. Moreover, FAKTUM will also support CATAI in designing its health application using the USB token, by supplying its professional Software Development Kit.

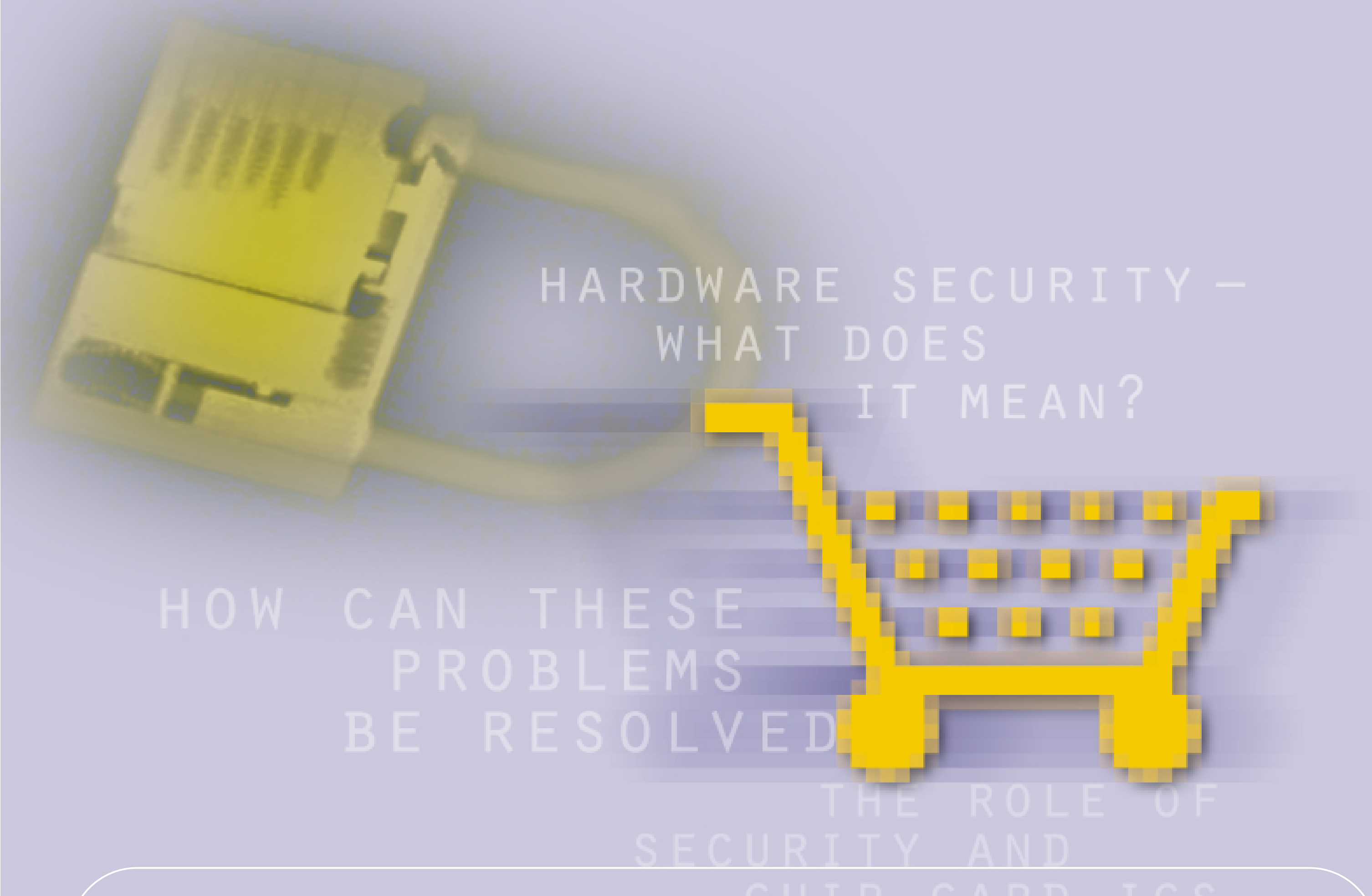
These developments are based on the proven components of the FAKTUM product CryptoSeal SDK and the e-finance application BankAround for the banking tests.

After a test phase of the hardware and software components within the e-banking area, executed by Dresdner Bank AG, and by CATAI for the e-health environment, the Smart USB token will be an affordable, highly secured and convenient alternative for the mass market in respect to hardware based identification and authentication means, as well as for financial transactions. It is hoped that the Smart USB token will open new ways for not only governmental and public authorities, and the health care sector, but also for the whole area of enterprises, e-business and e-finance. Due to the structure of the Smart USB token, it will be possible to use one single token as a means of identification and authentication for a lot of different, daily-life applications in need of convenient and the highest possible security - a security solution that really is covering the growing security demands of the future.

For more information visit: www.faktum.com



In recent years the term e-commerce has become the accepted buzzword, with huge markets predicted for this particular segment and the added bonus of large opportunities for a lot of companies. This growth ensures a successful future, as well as new, comfortable ways, of exchanging information and doing business over the net for private customers and organizations alike. However, e-business has changed. It is no longer the old view of e-commerce: "doing transactions on a PC". E-business is a way to conduct, manage and execute business transactions via an electronic network. The customer will use devices that they find more convenient. And while the convenience for the user grows, devices will get smaller and their functionalities will expand. At the same time network access becomes cheaper, and online attractions will also grow.



Hardware Security for e-business

By Monica Bremer
Infineon Technologies AG

The first period of Internet business focused on earning revenue through advertising (web banners) and numbers of users for network access. Customers today are used to getting online content and services for free – this will change in the future. The new business models and trends will concentrate on online education, high value content and personal services with the benefit of added value that the customer is willing to pay for. But up to now, these trends have not yet been realized. Everyone is prepared, a powerful infrastructure exists, but the mass consumers are not moving down the road of e-business.

The missing element is trust. Trust has always been the basis for conducting every type of business. Powerful guidelines for the electronic market place have to be established in order to give all involved parties a trusted key for doing e-commerce. Asymmetric cryptography, like public key cryptography, together with tamperproof devices for storing private keys, are the two basic components that will help to justify the hype of e-commerce.

Dangers and Risks

Making use of the Internet for e-business has the advantage of utilizing a widespread infrastructure as a physical basis for the electronic market place, at no cost. On the other hand, users have to struggle with security issues, as the Internet wasn't designed for commercial usage. From its origin there was no need for a security infrastructure, which means that people using the Internet for e-business have to face several risks. The first risk is one of confidentiality. By default, information traveling through the web is in plain text – an open book to nearly everybody. The idea that company confidential data involved in business transactions can be read by anyone, is a limiting factor for the use of the Internet. The second risk is that data integrity has to be assured. In the same way everybody can read transmitted information, it is also possible to change it. Imagine your salary is re-directed to Mr. X, just because he changed the number of your bank account to his. From this example it is clear that the question of authenticity is a crucial one. How can a person be sure that the web-page they're looking at, is from the organization that it is claiming to be? Last, but not least, the risk of 'denial of service' attacks could close down the doors of a cyber-shop and drastically limit its business.

How can these problems be resolved?

One of the main questions is "who is liable for ensuring that the e-business process is secure for the end customer"?
E-business applications using the Internet as a platform, have to solve the requirements for confidentiality, integrity, authentication and the question of non-repudiation. Since the Internet itself does not cover these problems, protocols and applications of the upper layers have to be designed in order to realize secure solutions. What does a secure solution really mean? The user needs to have the means for hiding the content of their transactions from the eyes of a third party. They need to have the possibility to check whether their partner is the one they claim to be (and by the way, the reverse also holds true). Both need the legally binding commitment to a deal, including a legally accepted signature and a certification of time stamp.

Since these are crucial requirements, legislation all over the world has dealt with this topic in the last few years, to offer a framework for common accepted solutions.

In the USA, Utah came up with a law for digital signatures back in 1996. California followed last year and several other federal states are preparing comparable laws. In Europe, Germany stated its digital signature law (SigG) in 1997. This was later specified more clearly by "Signaturverordnung" and "Maßnahmenkatalog" of BSI (Bundesamt für Sicherheit in der Informationstechnik). Its goal was to establish a framework, which allows the qualification of electronically signed documents to have the same legal authority as manually signed paper documents.

The technology basis for signatures should be the use of asymmetric key pairs for public key methods. The certification authority has the task to ensure that the digital ID, together with the private key, is securely stored in a security token. This practically implies the use of crypto Smart Cards. Other countries have followed with laws concerning digital signatory, such as Italy, Austria and Finland (who have started to issue personal ID cards with a digital identity). Work has already started on a European level in order to achieve a common approach to these issues.

Hardware Security – What does it mean?

Up to now there are some very specific basic requirements that have to be fulfilled in order to provide a strong basis for secure business over the Internet. Generally speaking, a chain of trust has to be built up between both customers and dealers. Modern cryptography, based on the public key infrastructure, together with a secure device to execute cryptographic functions and to store private keys, are the solution to these requirements. On an application level both the ease of use and the high level of security are crucial for the success of these solutions.

From the software point of view, a lot of improvements have been achieved in recent years. In the end, Internet applications became additional features, providing basic security mechanisms. IPsec (Internet Protocol Security) for network layer, SSL (Secure Socket Layer) or TLS (Transport Layer Security) for transport layer and SHTTP (Secure Hypertext Transfer ProtocolHyp) for the applications layer, are all techniques that deal with the different topics of confidentiality, integrity and authentication. These techniques are powerful tools to upgrade the functionality and level of security of the communication path from the home PC, over the Internet and into the server of the service provider. But in this process, both the transmitter of information and the receiver of the information, and their clear identification, play an important role. To build up the trust relationship, the combination of the personal identity and the digital one has to be guaranteed. In order to prevent misuse of digital identities, a security device is needed that operates separately from untrustworthy platforms (like a PC) and have the capability of storing keys in a tamperproof way, as well as performing cryptographic functions. Using such a security hardware token, the private key never leaves this sealed environment. Crypto controllers known from such products as Smart Cards, are ideal candidates to fulfill these tasks. In the non-volatile memory, private data and keys can be stored securely. The powerful crypto part of the controller can perform signature of hash values. The internal logic of the device allows access only by receiving the right PIN (personal identification number) from its user. With these two powerful capabilities, crypto controller based security tokens will be the first important part in the chain of trust from customer to dealer, and therefore one big enabler for e-commerce applications. Above all else, the user doesn’t have to bother about all the internal details, because the Smart Card manages all this work for the user. Thus the Smart Card is really a personal computer that is as simple as possible to operate.

The Role of Security and Chip Card ICs

As you have seen, the use of hardware security tokens follows the demand for a trusted end-to-end security process, by both the customer and dealer and by many upcoming laws for digital signature. The requirements for secure storage of keys and the performing of crypto functions like signature of hash values, are fulfilled by Smart Cards today. But it is the crypto controller that is the really important part in this process and there is no need for this to be embedded in a plastic card form factor defined by the ISO7816 norm.

Since the PC is the most important platform for e-commerce today and nearly every PC is equipped with a universal serial bus (USB), new so-called USB-tokens have arisen. They can achieve the highest level of security if they are supplied with a crypto controller. One further advantage of this solution, is that there is no need for an additional reader like a Smart Card reader. This would significantly save costs for implementation of solutions based on a USB crypto token.

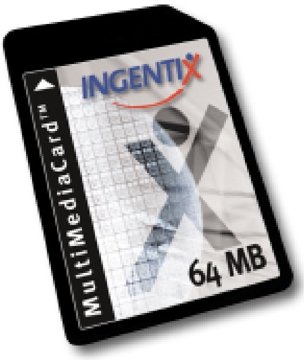
In the future, the dominant platform for Internet access will be mobile devices like PDAs or smart phones. As in the PC world, it would be best for a supplier to provide his customers with a personal hardware security device. As the mobile phones are developing very rapidly, there will soon be different possibilities to plug in such security tokens. But there are other solutions almost upon us. Within the year, we will have mobile phones from major players equipped with a MultiMediaCard™ slot. Whereas its original use is for functions like MP3 music players within the phone, secure download and so on, this is in fact a possible slot for a secure hardware token. Again, it is possible to integrate the technique of crypto controllers in the form factor of a MultiMediaCard™.

Hardware e-business solution examples

At the moment worldwide standards for e-business security are missing. So one can concentrate first on laws for digital signature in Germany and EMV (European Master Visa) requirements. Both require 32k EEPROM and 1.024 bit RSA cryptography. Infineon Technologies fulfills these requirements e.g. with the SLE66CX322P product. E-purse, digital signature and public key infrastructure are famous functionalities, often realized in a Smart Card form factor.

As we can see, the implementation in further form factors, or the building of multi-applications in combination with further products, result in different e-business solutions with their own particular advantage for the user.

Some Infineon solutions



MultiMediaCard™

The MultiMediaCard™ is a flash memory product for mass storage. Just create your own multi media terminal by the storage of different data, e.g. navigation, hotel and restaurant guides, dictionaries, mp3 music files, digital pictures, flight schedules and electronic books. Encrypted software can be stored without hardware security on MultiMediaCard™.

The implementation of the Infineon product SLE66CX322P on MultiMediaCard™ allows secure data storage without software encryption and, in addition, secures e-business within mobile devices. For example, one can use the mobile banking application or digital signature for e-business transactions and store the payment and transaction information on the Secure

USB Token

A USB token and a security controller are a powerful combination for performing security solutions. USB is a high-speed standard interface for PC and notebooks, required by the PC2000 specification. The security controller facilitates high performance crypto engines for DES, 3DES, RSA and HASH and a true RNG (random number generator). The Infineon product SLE66CUX640P as a single chip solution for USB Token supports USB 1.1 and performs as well with the requirements for digital signature, public key infrastructure and payment processes.

FingerTIP™

Convenience and security are driving factors for biometric solutions. Today the FingerTIP™ replaces the PIN and password. In addition, a person can be recognized and both features build a secure authentication with high user acceptance. Not only in Smart Cards but as well as in hardware, such as PCs, Notebooks, Mouse, Mobile Phones and PDAs, personalization and identification is possible.

For more information visit: www.infineon.com

The use of credit-card size Smart Cards has successfully been adopted by a number of European companies, with a particularly high level of acceptance in Germany and France. However, high hardware deployment costs and the lack of application standards associated with Smart Cards, have proved to be significant barriers to their widespread use, especially in the US. Therefore, their newly developed USB (Universal Serial Bus)-based counterparts (referred to as USB tokens) are becoming a more appealing, more versatile option for both American and European companies looking to secure their digital assets.

Smart Cards vs. USB Token And the winner is...?

By Charlie Hava, Solution Partners Program Manager, Aladdin Knowledge Systems

With strong user authentication based on similar Smart Card chip technology, USB tokens are not only more sleek, fun and convenient, but most importantly, more cost-effective than their budget-busting predecessor.

The strikingly obvious advantage to using USB tokens lies within its unique portability. Reader infrastructure exists in more than 90 percent of modern stations one would ever have to “plug it in to.” Virtually all PCs produced today have at least one USB port, whilst most PCs do not have a traditional Smart Card reader. In the past, the lack of Smart Card use could easily be attributed to the high cost of installing traditional Smart Card readers on PCs. Corporations’ unwillingness to even use or purchase extra card-reading devices contributed to the extremely low usage rate in the United States, as well as the extremely low popularity of the Smart Card format.

However, with the recent introduction of lower-cost readers, cost no longer poses such a significant barrier. So how do we explain the fact that traditional Smart Cards and readers are not present in all PCs? The answer is simple: service providers do not want to be responsible for the continual maintenance of these extra devices on PCs. The overwhelming issues related to logistics, customer support and the threat of PC problems and software complaints now prohibit the mass deployment of readers, and thus any widespread use of traditional Smart Cards.

Although USB tokens eliminate reader technology concerns and offer superior implementation requirements, the security offered in credit-card sized Smart Cards and USB tokens is quite similar. Both can perform RSA operations, authenticate and encrypt, offering very high levels of security. The Smart Card’s high security capabilities are anchored in its ability to perform sensitive operations inside the chip itself, thus providing a fully independent, secure environment. This is true in both the traditional Smart Cards and USB tokens. Functionality and security levels are virtually identical in both forms, leaving the USB infrastructure as an overwhelmingly significant advantage for tokens. Wherever a USB port exists, tokens can be quickly implemented. And tokens can be easily set up to supply secure log on, web access control for specific sites, as well as signing and encryption of email.

The evolution of USB token Smart Cards has been rapid over the last few years, beginning in late 1998 with the introduction of tokens that used, at best, secured EEPROM protected memory, technology that, at the time offered a less robust alternative to traditional Smart Cards. These tokens utilized a range of onboard crypto processors, mainly symmetric or hashing capable. Slightly more advanced tokens were then introduced that used onboard DESX (120 bit) symmetric encryption, similar in its key length to the encryption offered on Smart Card based technology. But despite this strong move forward, the keys did not offer any RSA capable chips, and therefore still required digital certificates and other vital information to be generated on the PC and then eventually transferred to the token. However, today’s advanced USB tokens now provide on-board PKI key generation similar to traditional Smart Cards providing equivalent security levels. But despite their identical high levels of security, USB tokens offer clear advantages not possible through traditional Smart Card use.

▶ **Deployment** ▶ As stated previously, traditional Smart Card implementations require external readers to be installed on each user's machine. For a company with just 1,000 employees, the initial reader hardware cost alone can be extremely high, not including maintenance and implementation time. The difficulties associated with the installation, management and actual deployment of Smart Card readers have given these readers a reputation for being repeatedly problematic. This significant, decade-long concern is addressed by the USB token's ability to authenticate users while using standard PC connectivity. No external readers are needed, and instead, the USB ports now available on virtually all PCs provide welcome relief to the headaches and hefty price that come with traditional Smart Cards.

The ability to use USB connectivity is especially significant for large-scale distribution of tokens, such as sizable e-commerce applications. By deploying reader-less Smart Card technology, organizations can minimize cost, while providing simpler implementation and fewer headaches. Customers and users more readily accept USB tokens primarily because they utilize the USB port infrastructure already available – something not possible for traditional Smart Card readers.

▶ **Portability** ▶ Although traditional Smart Cards fit nicely inside a wallet and are similar in look and feel to the typical credit card, USB tokens offer the convenience of being stored on a user's key chain. Significantly reducing the chance of losing or misplacing the token, this added benefit helps users easily integrate the token into their everyday routine. Users simply plug in the token when they enter their office or workstation and unplug when they leave.

Not only is physical portability important, but application portability is also a necessity. For both forms of Smart Cards, flexibility is provided through out-of-box plug-and-play connectivity to multiple business applications, including those based on CAPI and PKCS#11. In addition, Smart Cards integrate with a wide variety of network security clients and PKI solutions offering numerous options for organizations. Due to their two-factor authentication process, even if a user needs several user accounts and certificates, all the user must remember is the password. USB tokens with powerful two-factor authentication offer true peace of mind as well as ease of use – a combination well respected among companies of all sizes.

▶ **Durability** ▶ Another significant logistics-related concern is the proven life span of the hardware. Chips inside both USB tokens and traditional Smart Cards cannot be physically tampered with, and if they are altered in some way, most chips are designed to automatically destroy themselves. This is an added benefit provided by the chipmakers and has become an industry standard. But true durability assessments must also include readers. Readers, replacement readers, parts and the maintenance personnel, especially in sizable deployments, not only create long-lasting expenses, but also an added level of inconvenience that cast doubt on traditional Smart Card durability. Fewer parts, more durable usage criteria and simpler maintenance easily give USB tokens equal or great levels of durability.

▶ **Flexibility** ▶ USB tokens, and traditional Smart Cards, seem to offer similar application flexibility. Both utilize either a port or hub on a PC and some readers have more than one slot. Two significant drawbacks, however, remain with traditional Smart Cards. Most standard card readers have a maximum of two slots, while the reader itself is connected to an existing port on the PC, thus creating a potential pile up on the serial or parallel ports. By contrast, PCs now have defined a maximum of 127 USB devices per machine, far outnumbering the traditional Smart Card reader capacity and opening great potential for USB technology. Combined with the USB token's ability to store multiple digital certificates and credentials, the PCs capacity for 127 USB devices offers far greater flexibility than the traditional Smart Card.

Though USB tokens are still an emerging standard in the authentication market, their many advantages are quickly gaining widespread acceptance in the US and Western Europe. When compared to traditional Smart Cards, as well as biometric devices and one-time passwords, USB tokens offer unmatched levels of security, while also providing much-needed portability, ease of deployment, PKI support, multiple application support and durability.

For more information visit:
www.ealaddin.com

Protected Storage Devices

By Loqware Technologies AB

Every day, millions of professionals and executives are traveling across the world with confidential information contained within their portable computers. The loss or theft of a laptop, or rather the content of it, can render substantial damage, resulting in severe consequences to any organization. Corporate planning and classified data, client information, passwords, account numbers, personal secrets, e-mails and more may become exposed.

The LoqDrive™ 250 series from Loqware offers a truly unique, mobile storage solution to ensure that this sensitive data is kept private! The vital information stored on the hard disk is protected from being accessed, even by co-employees or family members when the authorized user is not present.

Both laptop and desktop computers are more or less constantly accessible by other employees, network administrators, system consultants, temporary co-workers, and of course thieves, who can all physically touch and manipulate the storage media. Actually, several surveys indicate that as many as 70% of all computer security breaches are executed within a company by its own personnel.

Most security products available on the market today, like advanced encryption applications and user authentication products, have clearly contributed in providing reasonable security. They do not, however, efficiently protect data from attackers who already have access to a computer or its hard disk drive. Software encryption solutions are limited by different factors, like a poor operating system or PC platform security, the complexity of integration in systems or degradation in computing performance. Hardware encryption products are typically expensive and rarely suited for use with laptops and portable storage devices. The user also has to accept the choice of encryption system supplied by the hardware manufacturer. Moreover, additional risk factors with encryption are related to how and where the encryption keys are stored, the threats of exposure of PC viruses or Trojan Horses, and not least, bad handling of the encryption keys by the users. With these impending risks, it becomes necessary for complementary security functions.

Many skilled crackers can, if they are given the time required, bypass the operating system's security mechanisms and even derive encryption keys or other information from temporary or swap files once they have possession of a disk drive. However, such advanced techniques are completely unnecessary in case they find all required security Dongles, Smart Cards, access codes notes, and other security devices that are often kept close to the computer. And with sufficient personal knowledge about the user, they may even have a fair chance at guessing the passwords.

As long as the attackers are able to access the computer equipment directly and physically, the criterion for protection has to be dramatically sharpened.

It becomes necessary to deploy stronger security defenses that assures data integrity and keeps the critical data from being revealed or modified.

The users constitute another major problem by themselves. Firstly, most users are not at all aware of the high monetary value of the information they carry. Secondly, they tend to be oblivious to the fact that they expose their employer to unnecessary risk by their negligent behavior or habits.

Loqware has developed a complete mobile storage system that provides vastly improved protection against unauthorized data access, even when the attacker has possession of the disk drive and perhaps, in the worst of cases, even access to a clean laboratory room for disk data recovery activities.

As a new solution to protection of high-value data, Loqware launched the first security product of its kind in the world, designed specifically to protect the hard drive and its contents by using a self-contained fingerprint recognition and protection system.

The first member of a family of secure disk storage products is the LoqDrive™ 250 SPR, a disk drive for mobile use that combines biometrics and encryption without the need for passwords or security Dongles. Sensitive data can be transparently stored on the disk without requiring any changes to application software, O/S drivers, or other security applications. The LoqDrive 250 SPR offers the mobile professional one touch sign-on convenience and state-of-the-art security at an affordable cost. In addition, it's protected from the elements inside a tamper resistant, ruggedized and lightweight aluminum housing in a compact size.

The LoqDrive 250 SPR may also be used for high-speed transfer of data between two computers or as a back-up unit. Most importantly, in the event the unit is lost or stolen, the disk data will still remain access-protected and unreadable, defying the most sophisticated attempts of intrusion.

The LoqDrive 250 SPR consists of a 10 GB hard disk drive that is connected to a PC supporting the USB1.1 interface. A biometric fingerprint sensor is integrated and fixed to the disk drive body. After a successful user verification process, it will behave just like another disk drive and will not interfere with either the operating system or any standard application. It can also be combined with other security applications to maximize the level of data protection. If an authorized user is not successfully verified, the LoqDrive will remain locked so that absolutely no data can be written or read to the disk platters.

The choice of a biometric authentication system is motivated by the fact that it ensures a non-transferable function which requires the confirmation of an individual's physical presence, thereby preventing anyone but the correct user (or users) authorized by an administrator, to be given access. It also replaces the need of personal passwords, PIN numbers or other logon codes, which often causes supplementary overhead costs for the corporate IT-department.

In addition, the Loqware i-Loq™ protocol secures all communication between vital internal electrical components, like the fingerprint authentication module and the hard disk controller, so the keys are never exposed to measuring or replaying of signals.

Several users can be enrolled on the LoqDrive 250 SPR. It works independently of any host software and can be connected to any computer platform supporting USB. There is no adverse impact on the computer systems performance or disk speed.

All LoqDrive models come bundled with a suite of security software including LoqFolder™, which is an advanced encryption software allowing the user to individually encrypt and decrypt files, folders and applications using the Blowfish algorithm with a 128 bit key. Folders on the system can be locked on a user-by-user basis, which makes it possible for multiple users to share the same disk drive or computer platform without access to each other's files.

The market for the LoqDrive 250 SPR product consists of virtually all users who are most concerned about securing the integrity of their precious information, especially when they are "on the road".

These customers span across a wide range of industries or areas, such as Biotech & Pharmaceutical, Technical R&D, Governmental Authorities, Military & Police, Banking & Finance, Management Consultants, Law Firms, IT-consultants, System Developers, Network Administrators, Construction Industry, Industrial Designers, Automotive Industry, Universities & Educational Sector, Press & Media, etc.

For more information visit: www.loqware.com

By Derek McDermott, Managing Director Informer Systems LTD

Securing Computer Peripherals using Biometrics

A look at the different solutions on offer today: mouse, keyboard, and hard drive. How these can be implemented, and the business implications they will have.

In an age where information has become the new currency, it is has become more critical that we can guarantee ways of preserving this valuable commodity, using the best technology available. With the full impact of the Internet over the last decade, the strategic relevance of e-business for future revenues is now being acknowledged, but in order for this to flourish, the user needs to have confidence in purchasing goods and services over the World Wide Web. This position can only be achieved by providing proof of the Internet's inherent security and the belief that a user is not going to be exposed to some kind of fraud - whether it is the theft of highly sensitive credit card information or even the risk of personal bank details being publicized on the Net!

In the past, it has been difficult to counter these arguments, because the tools that were being used to identify the user were woefully inadequate and open to sabotage. It is now widely admitted that the use of passwords gives little confidence to the user. Not only is it easy to crack passwords, but also 'do-it-yourself' hacking programs are freely available to download on the Web itself. Not only is the concept of password-protected access fatally flawed; the cost of supporting such a system is considerable. The majority of computer support departments freely admit that passwords are a time-consuming business, with 65% of IT support calls relating to lost passwords or user errors.

With the introduction of strong authentication whereby a user offers up more than one source of their proof of identity, the confidence in the quality of secure access has risen, but it still does not guarantee absolutely that the person logging on, is physically present. Biometrics promised to address this, in a bid to provide a hassle-free and accountable way of establishing that the user is, who he or she claims to be.

So what is biometrics, how can it be implemented and what are the benefits for the Business World?

Understanding Biometrics

Biometrics is the means by which an individual positively identifies himself/herself with the use of a physical attribute that is unique to them. So biometrics in its current developmental state, enables the use of a variety of attributes that can include: fingerprint, hand scan, iris scan, facial geometry and voice recognition. The use of a fingerprint represents the most significant in terms of adoption so far, at 34%*. A person's fingerprint is totally unique to them, and will never change, so is recognized as one of the most reliable of all the physical attributes in terms of matching up reliably.

Over the last five years, biometrics has really gathered momentum and has been heralded as an unequivocal means of ensuring that only authorized persons are given access to particular sources of information.

Research from IBG shows that the rise and influence of biometrics is set to continue. In 1999 total revenues derived from the biometrics market stood at $58.4million. The projected revenue for 2003 stands at $594million – an anticipated growth of at least 1,000 %. One of the major factors for this rate of growth lies in the pricing of the technology. For instance peripherals for finger scanning that may have cost $500 two years ago can now be found for under $100, making biometrics affordable for even the modestly sized business.

The Building Blocks of Biometrics

So let's look at a whole process of building a biometric solution for a range of different applications and consider the compatibility and integration issues that must be addressed.

For securing access either to remote (e.g. web server) or locally held resources (on your local network), you will need to consider the compatibility of your existing IT infrastructure with the choice of biometrics solution. What ISL (Informer Systems) provides is the software that acts as a 'bridge' between the biometric hardware and the infrastructure that holds the information that is being accessed.

ISL's SentriNET software range for example, incorporates biometric authentication and verification techniques to secure network access, by replacing the logon password with fingerprint authentication. The problem facing businesses is often a question of compatibility between the peripheral device and the network itself. This is where the ISL software comes in. Because SentriNET is based on an 'open' platform and can be embedded into an organization's current Netware and/or Microsoft user management programs, it makes SentriNET the simplest product to install and deploy with the minimum amount of user and administrator training required.

For the first time a technology has emerged that has improved not only security to the network and applications, but also improves the user's experience of access. The problems of compatibility though, are not solely linked to the existing infrastructure, but also relate to the choice of

*According to independent analyst, IBG (International Biometric Group) the current biometrics market comprises: Fingerscan (34%), Hand Scan (26%), Face Scan (15%), Voice (11%), Iris Scan (9%), Signature Scan (3%) and Retina Scan (2%)

peripheral that is being used. With most authentication software, the user is tied to using a specific peripheral. This is not the case with a product such as SentriNET that can work with all types of peripherals from various manufacturers (see later). The beauty of using non-proprietary software in conjunction with a biometric device is the staggering ease of use. So what's behind the operation and how does it work? Fingerprint templates created using the pattern of ridges and valleys that make up an individual's fingerprint, at the enrolment stage, are stored as an attribute of a user's user account. This could be in a database on the network or web server. For example with network logon, storage of templates is taken care of using the standard databases provided in the most common operating systems e.g.Security Account Manager (SAM) database in an NT4 environment, the Directory in Novell (NDS) and Windows 2000 Active Directory Server (ADS) environments, or on a Smart Card or similar personal storage device. A live fingerprint capture is then authenticated against these stored templates during the logon process, and access to the network is either granted or denied depending on the result of this authentication attempt. These templates are encrypted and stored either as a database record or on a secure part of the network.

So this is the basic procedure that is followed and we will later examine more closely, the choice of biometric add-on tools that can be used to read the fingerprint in the first place.

However, at this stage it's important to recognize that the technical set up differs slightly depending on the type of resources being accessed.

The Types of Secure Access

Network Log-On

ISL's SentriNET software is designed for network logon. After submitting an initial password, a new user enrolls by providing a scan of their fingerprint. Many hardware devices incorporate scanning facilities for developing fingerprint templates and by using a product such as SentriNET the user is not tied into using a particular one (see later). SentriNET requests the user to provide multiple copies of their fingerprint, in order to improve the reliability of the fingerprint if it becomes damaged in any way. Instead of requiring a separate server to store the templates, SentriNET can leverage existing directory services. This is less expensive for two reasons. Firstly there's no need to invest in a dedicated intermediate server for logon, and secondly there are none of the associated costs that would be required to maintain the integrity of this data. Alternatively the software supports Smart Cards for storing the digital template, enabling steps to be taken when the card is inserted or removed e.g. log the user out or suspend the session to a screen saver.

Costs are further reduced, as there is no need for additional Management. SentriNET extends existing network management tools, eliminating extra expenditure and minimizing the level of training. Again, because the biometric software is using the architecture of the existing operating system, templates stored in the directory are replicated and backed up as part the daily operation of the network.

Securing Remote Access to a Network

With ISL's SecurDial software token, users working from home or 'on the road', can remotely connect to a company network from wherever they are. SecurDial works in conjunction with ISL's Secure IT 3000 authentication server that grants access at the point of entry to the network. Again, ISL supports fingerprint recognition, avoiding the need for hardware tokens. Like the SentriNET enrolment process, SecurDial is straightforward to use. The user simply clicks on the SecurDial icon, scans their finger and connects. The software can be installed in any Microsoft 9x, ME, NT or 2000 workstation.

Once a user is logged onto a central network, it is now possible to control what applications are available to which users. Therefore further demands for fingerprint submission may be given according to the application required. For instance designated personnel, who would need to present a fingerprint reading before access was granted, may only access confidential financial information.

The only decision that is left for the network manager is the choice of tool that will scan the fingerprint for verification. Costs have diminished on all fronts with less training, less equipment and less storage capacity – a single template can take up as little as 128 bits of memory!

Extending Secure Access to the Web

ISL's eSentriNET uses the same principles as SentriNET, but provides biometric access to Internet or Intranet services, requesting fingerprint authentication when a secured web page is accessed from a browser. The implications of this technology are immense in terms of promoting greater uptake of world-wide e-business applications, enabling deployment of 'on line' web based applications where security is paramount, e.g. Financial Services, Healthcare, Human Resources, Application Service providers (ASPs) etc.

ESentriNET can be installed in all of the well-known web servers such as Microsoft IIS, Netscape or Apache and is compatible with the World's most commonly used web browsers, Microsoft Internet Explorer Version 4+ and Netscape. The user profile is stored in the Web Server or local directory services. ESentriNET provides all the advantages of SentriNET, yet because of the sheer dominance of web based solutions, is likely to boast a greater potential number of applications in the future.

For instance it is anticipated that large scale web based projects will often exceed a million users, a feature that eSentriNET is prepared for – with the ability to support any ODBC compatible database for template storage.

Now that the software requirements have been explored for the different scenarios, let's take a look at the biometric hardware that is currently available.

Spoilt for Choice

In the last few years the choice of biometric tools, especially for fingerprint recognition has mushroomed. Standards governing biometrics have matured and the price of devices has plummeted. Using non-proprietary software such as SentriNET, e-SentriNET or SecurDial, means that users are not forced into buying a specific product. So what ranges of products are available and what advantages can they deliver?

Integrated Keyboards

One of the most practical and logical solutions to opt for is a keyboard with a built-in scanner, as they take up no more room on the desk than a conventional keyboard and often provide a Smart Card reader as well. One of the leading suppliers of these specialist keyboards is Cherry who manufactures a range of keyboards designed for a choice of operating systems such Microsoft Windows 95/ 98/ NT4/ 2000. The keyboards comprise 104 keys, 43 of which are programmable. As the volume of biometric keyboards has increased, the unit cost has fallen to an average of $120, making it an affordable option for the majority of businesses.

Mouse

Another peripheral that takes up little additional space, the U-match® Biometric mouse has a patented fingerprint scanning methodology that is tightly integrated into a standard two-button mouse. Advanced optics and scanning methodology allow the U-match® mouse to generate a superior image. Unlike other commercially available mouse-based input devices, the U-match® biometric mouse does not capture the finger image and scrambles the algorithm at the point of scan. This methodology offers a superior level of security and an un-matched level of privacy. The Biolink mouse can be used on any network PC running Windows 95/98/NT4 or Windows 2000. For USB connectivity, Siemens' ID Mouse ensures full interoperability between the mouse and your PC, and as a result all available PC interfaces can be accessed for further applications. Used with SentriNET it provides login and screensaver support for any network PC running Windows 95/98/NT4 or Windows 2000.

USB Peripherals

There are many USB compliant solutions available, all of which are relatively compact. The credit card sized Sony FIU-710 scans, matches and stores fingerprints internally. The host PC or network server need never store the data, making the unit more secure. Additionally, this tamper-resistant USB peripheral is a PKCS#11 compliant hardware token, able to generate and store up to 1024-bit RSA key pairs via an onboard exponent processor and 512k of flash memory. The Sony FIU-710 can be used with SentriNET on any network PC running Windows 95/98/NT4 or Windows 2000.

Another option is the Precise Biometrics PB 100a and PB 100sc that plug into the PC's printer or USB port. The PB 100 is a very compact desktop fingerprint scanner and the PB 100sc supports an internal Smart Card reader to allow storage of the templates to a PCSC compliant Smart Card.

Other Options

For a low-cost fingerprint reader, SecureTouch® 2000 is a mouse-sized scanner that delivers easy-to-use security for computer and network access control. The parallel port interface, with pass-through adapter, allows it to work with SentriNET on any network PC running Windows 95/98/NT4 or Windows 2000. Login and screensaver supported.

All of the above solutions are fully compatible with ISL's SentriNET and SecurDial range, enabling trouble-free installation at an affordable cost. Although the most mature of the biometric methods is the use of a fingerprint, the architecture of SentriNET allows for additional devices to be added and for other types of biometrics to be used, e.g. voice or face recognition.

Once biometrics has been fully adopted, companies can begin to reap the full benefits that this foolproof technology can bring.

The Power of Biometrics

The impact of applying biometrics delivers improvements in security, which in turn leads to commercial rewards. From a network manager's perspective, biometrics solves many IT headaches for the support department. By liberating themselves from the time consuming tasks of supporting inferior security such as passwords, IT personnel can concentrate on more productive matters such as network planning or developing new applications. IT help desk calls where users have locked out their accounts because they could not remember passwords are virtually eliminated. At the same time, the cost of password administration is drastically reduced and the technology is straightforward to install and requires little training.

Someone is Always Accountable

However, perhaps the most critical benefit that the network or IT manager enjoys is 'peace of mind'. Biometrics is the first technology of its type to positively identify an individual, therefore eradicating the risks of illegal hacking, and the prospect of data being misused or even stolen.

This aspect of biometrics forms the lynchpin of secure transactions over the Internet.

Until now, certain industries where confidentiality is paramount have been tentative over instigating web-based biometrics because of the concerns about security.

The ubiquity of Biometrics

Now it is conceivable that all types of industries will embrace biometrics as a means of legitimizing e-business, regardless of the sensitive nature of data involved. Therefore all types of organizations such as banks and government agencies that previously shied away from web-based communication, will be able to defend accusations of possible breaches with the powerful arguments of biometrics.

In the future, it is envisaged that a person's physical attributes, be it fingerprint, iris, retina or voice, will replace items such as credit cards or passports. After all, it is difficult to lose something that is omnipresent. This suggests that like a person's fingerprint, biometrics is set to become a permanent feature in all walks of life. As the technology continues to come down in price, the ubiquity of biometrics will be secured.

The explosive growth in remote access applications and subsequent need for secured electronic data transfer across corporate networks and the Internet has developed a substantial need for secure user identification and authorization. The sophisticated technology available to today's professional hacker means organizations can no longer depend on conventional methods of userid/password access control.

Biometrics is becoming the 'norm' for not only large applications and projects, but also for protecting access to individual computers, cell phones, pocket sized personal computers, networks, web servers and database applications.

ISL designs, develops, manufactures and markets software products for the capture and comparison of biometrics, such as fingerprint, and/or smart card for security applications including Network Access, Remote Access, Web Access and Database Access. Established in 1989, ISL headquarters are in Bromsgrove, Worcs, in the UK, and ISL markets its products through authorized reseller and OEM channels.

For more information visit: www.informer.co.uk

No, there's nothing dull or mousy about the new ID Mouse Professional from Siemens – neither visually nor technically. Of course it's the visuals that grabs your attention first - a sophisticated design for a PC mouse, with elegant lines in blue and silver. It feels comfortable in your hand, and would look good on any desk. And the technology? From either above or below, the ID Mouse Professional offers you the latest in biometric and optical technology.

Security that's FUN

High Tech Mouse for Professionals

By Stefan Kuhn, General Manager of Biometrics at Siemens AG

As early as three years ago, Siemens was one of the first companies worldwide to announce a terminal device with biometric functionality: the ID Mouse with an integrated FingerTIP™ sensor from Infineon, which attracted a lot of attention internationally. The ID Mouse Professional that has now arrived on the market is the continuation of Siemens' biometrics market strategy. Fingerprint recognition, a biometric process that is particularly well accepted by users, has been integrated in an innovative PC periphery device. The goal is to make biometrics as easy for the user to handle as possible – the ID Mouse Professional's simple operation and attractive design are meant to be fun to use. Market surveys show that security solutions are accepted only when they do not make the user's work more complicated than it already is. On the contrary, the ID Mouse Professional simplifies many things. Instead of having to keep track of PINs and passwords, the user just lays a finger on the biometric sensor to unlock his/her local PC, or to gain access to the company's intranet or to a marketplace in the Internet.

There is hardly any other device that the PC user uses as intensively day after day than the keyboard and the mouse. The ID Mouse must therefore be well accepted as a device. The most innovative feature is, of course, the optical movement sensing, which differs from the traditional mouse ball, in that it is completely wear-free, and works much more precisely on practically any surface. An ergonomic scroll wheel makes navigation easier, especially in the Internet, and the ID Mouse is of course suitable for both right- and left-handers. Not only is the housing attractively styled – it is also available in two color variants, light blue and silver-blue.

Development of the biometrics functionality of the ID Mouse Professional has, of course, continued. Improved algorithms have lowered the False Rejection Rate even farther to the rarely-achieved level of 1.3 percent, with a False Acceptance Rate under 1:1,000,000. And the time taken for authentication is only half a second. For the user, this means that the ID Mouse Professional recognizes the authorized user very quickly and very reliably. Any attempts at tampering are automatically recognized by means of a memory function that denies access as soon as the sensor registers an absolutely identical fingerprint more than once.

The first use of the ID Mouse, enrolment, has also been further simplified. As with any biometrics application, reference data must first be stored, so that – in the case of the ID Mouse – it is possible to compare fingerprints in an operating situation. The ID Mouse Professional software provides optimum support for enrolment, so the mouse can be initialized quickly and easily, even by less experienced users. Thanks to USB, installation of the device and the necessary driver also present no problems. Actual enrolment can first be practiced in so-called play mode. Here, users receive feedback from the software about how to position their fingers on the capacitive sensor in order to store the

optimum result. This direct feedback – for example, the instruction to press the finger more firmly on the sensor – means that enrolment is only a matter of a few moments. And, if the user wishes, enrolment can be carried out for each finger separately.

In the user administration of the ID Mouse Professional, which can be used under Windows 98, ME, NT and 2000, the administrator can define several users for one PC. In the case of Windows NT and Windows 2000, the user, after laying a finger on the mouse, is automatically granted access to the domain that has already been defined for him/her in Windows. If desired, the fingerprint can also deactivate the screen saver during normal operation. Specially developed software also allows the passwords for protected local applications and files to be replaced by fingerprints. There is also a software solution to allow additional network functions, giving the user convenient, secure access to programs and files within the corporate network. This is also available to mobile users (Remote LAN Access). Managers on business trips, tele-workers or field-service employees can thus access their own resources – like files or e-mails – with the ID Mouse Professional and their fingerprint.

All this shows how simple it is to integrate the ID Mouse Professional in existing infrastructures, or in a company's security concept. Customizing can be carried out without any knowledge of biometrics, using the ID Mouse Software Development Kit (SDK). For example, the ID Mouse Professional offers the capability of integration in Smart Card solutions. This involves the users' biometric data being stored in encrypted form on his/her personal Smart Card. On the one hand, this solution is particularly secure, because the biometric data is stored only on the card, and are therefore always under the user's control. The so-called matching-on-card technology is used. This means that the card contains not only the templates but also the biometric algorithms for comparing the reference data with the biometric data currently being read in, and that this comparison takes place in the secure area of the Smart Card. On the other hand, the use of Smart Cards means greater flexibility, because the users can simply login at any PC within the company's network that has a Smart Card reader and an ID Mouse. An example of further uses that could be integrated in this system, would be access to company premises, where Smart Card and fingerprint could positively identify the employees.

In e-commerce, it is also possible for users to authenticate themselves unambiguously by a fingerprint, and thus gain access to special offers in the Internet, for instance. For several months now, the Webtradecenter (www.webtradecenter.de), the largest German B2B market place for information technology, has been offering its members the option of identifying themselves using the Siemens ID Mouse and their fingerprints. And of course, internal processes can also be simplified in a similar manner, with travel expenses applications or internal orders being confirmed by a fingerprint.

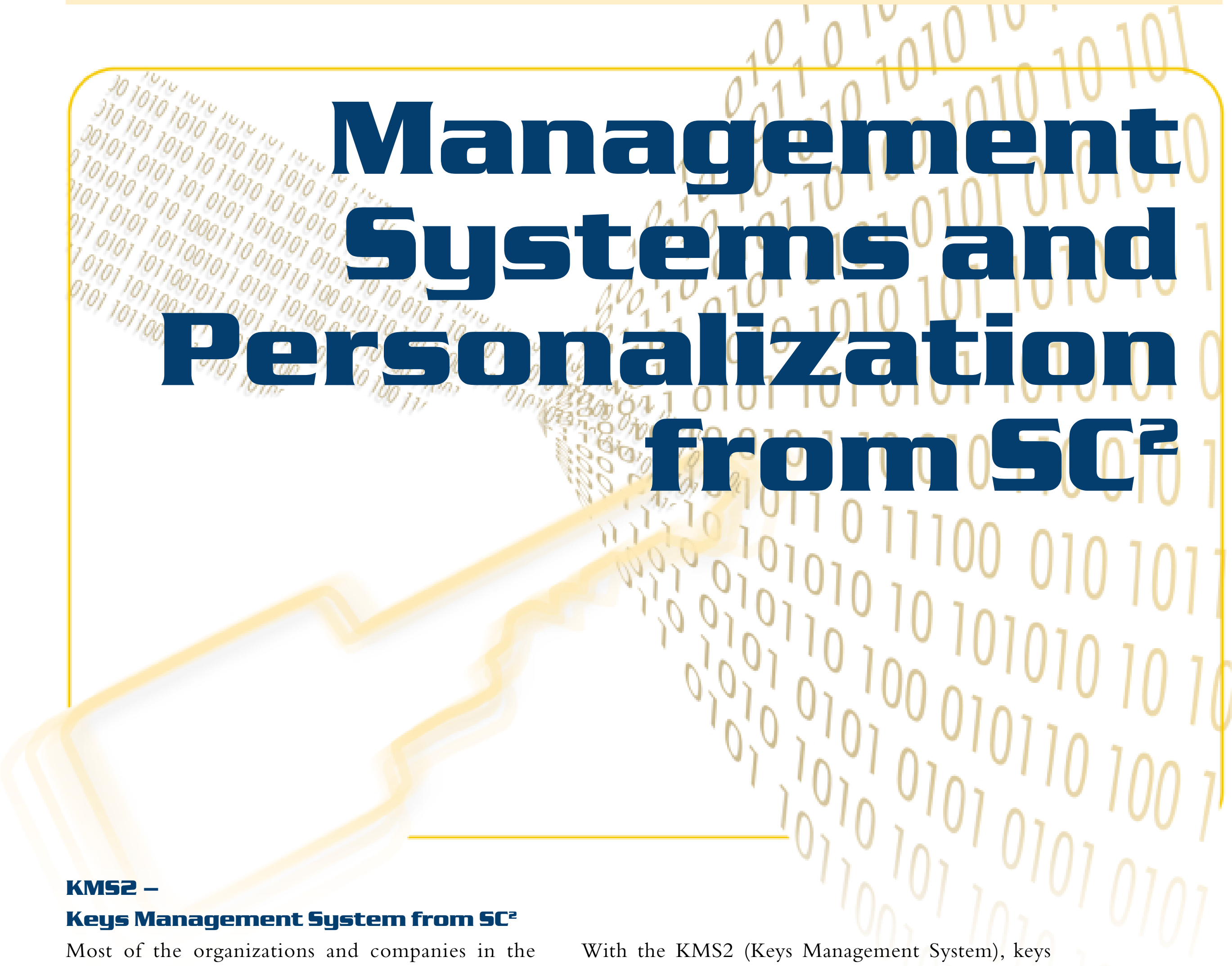
In any case, Siemens takes data protection very seriously. This is important for security reasons, but it also significantly increases the users' acceptance of biometrics solutions. With the ID Mouse Professional, they need have no fear that biometric data will be stored in such a way that it can be misused. To further increase security, the reference data is stored in a heavily encrypted format (DES3). Depending on the security concept, this can be done locally (the usual method), or the biometric data can be administered centrally within a network or stored on a Smart Card, as mentioned earlier. In any case, the biometric reference data and the user data are stored separately and encrypted.

The decisive aspect for the user is, of course, that handling the ID Mouse Professional soon becomes intuitive, and is completely trouble-free. In daily use, it takes some of the load off the PC user. Quick login to the system without having to wrack your brains for those bothersome passwords, and the very convenient mouse functions, ensure that the ID Mouse Professional is fun to use. Its styling certainly plays a part in this, too.

ID Mouse Professional: The Siemens ID Mouse Professional offers a maximum of security and convenience for login to PCs, networks or web-based e-business solutions.

For more information visit: **www.fingertip.de**

Management Systems and Personalization from SC^2



KMS2 –
Keys Management System from SC^2

Most of the organizations and companies in the world protect their IP (Intellectual Property) by using different cryptography mechanisms. These cryptography mechanisms are based on PKI (Public Key Infrastructure). Only in highly secured systems are both hardware and software used - many security solutions include a hardware device that protects the system keys, as well as software and hardware mechanisms that protect the transactions/communications, but a lot of those solutions do not include a proper key management. Today most of the organizations that implement a PKI solution, put their effort only in the protection of the CA private key and don't pay attention to the CA key Pair Generation, storage and Key Recovery, and therefore reduce dramatically the security level of the system. In software based PKI solutions, keys are vulnerable, since they are generated and stored on servers or PCs with a standard operation system, which don't include proper security counter measures. If the CA private key is compromised in a PKI system or a Master key in a secret system, then the overall security of the system can break down.

With the KMS2 (Keys Management System), keys are generated, stored and managed in a highly secured environment and tamper resistant hardware. KMS2 allows the generation of keys for secret key systems and PKI projects, and then provide full control over each step and each key without compromising security.

This system also provides a very powerful tool to manage the key's life cycle on variant platforms. KMS2 is fully controlled by hardware (Smart Card system and/or biometric mechanism), which provides a high level of security, as well as providing transparent keys backup and recovery in order to provide the organization with backup system keys, and a keys recovery policy. KMS2 supports different secret key sharing techniques and can be integrated into any system and adaptable to any proper keys management (definition, implementation and maintenance).

KMS2 can be combined with root Certificate Authority (CA) and supplied to System providers, Integrators, Organizations and End users.

SC² Smart Card personalization system: SC²@personalization

Integrators and project managers in the Smart Card information security field are aware of the fact that in complex projects such as: Health, Banking, and Governments etc, the databases are wide, diverse and change on daily/weekly basis. SC² is able to satisfy their customers' needs throughout the personalization stages, link to different databases in a secure way, provide the customer the flexibility in mapping for different needs and update the databases. This is because SC² has a flexible personalization system, designed to handle complex projects, and enables the customer to create a solution in a major stage of the project and in the life cycle of the cards. The system provides a solution not only for personalization projects that work sequentially, but also for the demand for particular services, such as a fast modification process, the need to prepare infrastructure for additional information that is to be added in the future, as well as assorted needs of the customer in different fields.

SC²@personalization is the most advanced, universal customizable system of its type, suitable for the contact and contactless Smart Card. The platform is flexible with most environments and employs a user-friendly graphical interface, based on OLE DB technology, which ensures easy access to most of the databases and applications.

The issuing station provides support for a vast amount of scripts, and offers flexibility to the user, with the option of adding special script applications.

The unique characteristics of the system are:
a) Reliability check of information by an internal cryptographic system
b) Creation of a log for user needs
c) Variety of mapping possibilities
d) Automatic database updates

The SC²@personalization system adapts the personalization system to fulfill the different customer's applications and needs.

About SC²

SC² Ltd. a subsidiary of Nisko Project Electronics & Communication (1999) Ltd. SC² is a leading Smart Card solution provider. The company offers a wide variety of solutions to meet the varying needs of customers, including contact, contactless and dual-interface Smart Cards. SC² has a team of talented and experienced security architects and engineers. SC² has experience with real worldwide implementation of Smart Card technology and designing state-of-the-art cryptographic algorithms tailored to the specific customer requirements, for the following applications: GSM, Internet secure access, Transportation, Banking, Healthcare, Gambling, Identification, Loyalty, Parking meters, Electricity meters, Sport, Communication, M-Commerce, Prepayment systems.

Solution Provider

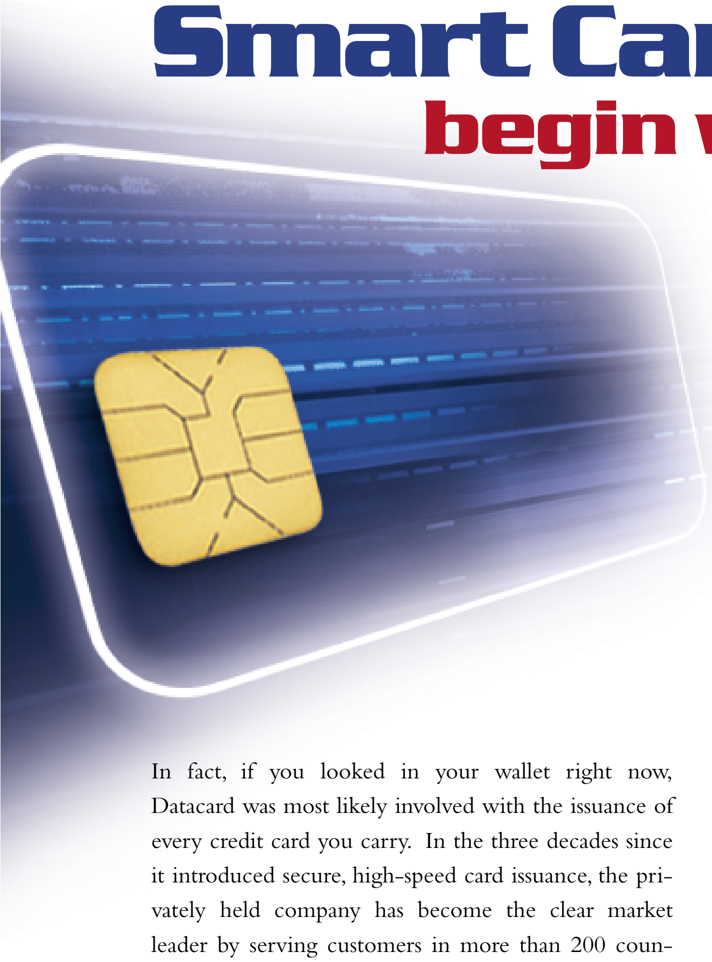
- Developing entire Smart Card systems
- Contact, Contactless and Dual-Interface cards
- Develop customized Smart Card Operating System
- Apollo - Smart Card Operating System
- OEM software and hardware to integrate Smart Card technology
- Building software and hardware to integrate security technology
- Cryptographic architectures and applications design
- Secure electronic commerce applications and protocols
- Make feasibility tests and loyalty schemes
- Distribution schemes
- Authentication process
- Personalization process
- Secure production process
- Database protection
- Security Embedded systems
- Secure Data communication
- Keys Management System (KMS2)
- Secure File – File & E-mail Encryption System
- Secure Logon – PC Access Control

For more information please contact:
Jacob Mendel / V.P. R&D and Security
SCsquare Ltd.
2A Habarzel St., Tel-Aviv 61580, ISRAEL
Tel: +972-3-765-7-331, Fax: +972-3-765-7-333
Mobile: +972-54-54-7-369
E-mail : jacob_me@netvision.net.il

SC² TM Ltd.
Security Chip & Communication

www.scsquare.com

Successful Smart Card programs begin with Datacard



Datacard Group helped transform the world for consumers and card issuers 30 years ago by enabling secure, high-volume issuance of magnetic stripe-based financial cards. Today, a vast majority of the world's financial cards – along with many other plastic cards used for other transactional and identification applications – are personalized with Datacard® systems and software.

In fact, if you looked in your wallet right now, Datacard was most likely involved with the issuance of every credit card you carry. In the three decades since it introduced secure, high-speed card issuance, the privately held company has become the clear market leader by serving customers in more than 200 countries. Recent expansion includes new software development centers in the U.S., U.K., India and Japan.

In addition to financial card issuers, Datacard provides corporations, government agencies, telecommunications companies, retailers, transit agencies, service bureaus, colleges, universities, elementary schools, insurance companies and healthcare providers with the systems, software and consultative expertise they need for successful card programs.

Today, Datacard stands on the brink of an even greater global transformation. In collaboration with the world's leading financial institutions and other leading Smart Card technology companies, Datacard is the only company to have developed an end-to-end infrastructure for personalizing, issuing and managing multi-application Smart Cards.

The Smart Card age is upon us. Tremendous market opportunities await consumer marketers, financial institutions, corporations, government agencies and other card issuers who can quickly and expertly bring this powerful technology to market. Datacard offers the proven skills and experience card issuers need to launch and maintain cost-effective, profitable programs.

Datacard's Smart Card portfolio features a secure, highly productive infrastructure for personalizing, delivering and managing multi-application Smart Cards. This infrastructure is more than industry leading software and hardware components. Its real value rests in perfect integration. Every aspect of this infrastructure — from Smart Card operating systems to server-based personalization managers to life cycle management systems — are designed to work together seamlessly. As a result, Datacard is uniquely positioned to help card issuers implement Smart Card solutions that are scalable, expandable, productive and cost-effective.

Critical elements of a quality Smart Card infrastructure

Only Datacard offers all the hardware, software and services components necessary to capitalize on emerging Smart Card opportunities. Each solution reflects Datacard's commitment to open architectures and scalable designs.

▶ **Smart Card Operating System**

The Datacard® Aptura™ Smart Card Operating System provides card issuers with complete control over costs, risk and the direction of their Smart Card program. Aptura is an open software product based on the Java CardTM 2.1.1.and Open Platform 2.0 specifications. For ease of use, it comes pre-installed on a chip and ready to drop into card plastic. By using globally recognized standards, the Aptura system provides a highly stable applet platform – and it supports post-issuance management of applets using a card life cycle management system such as the Datacard® Affina™ Platform Management Architecture.

The Aptura system also offers the long-term flexibility issuers need to attract and retain cardholders. A flexible framework makes it easy to add or update applets after cards have been issued, so issuers can offer their cardholders fresh, new products and respond quickly to their wants and needs.

In addition to strong product differentiation, the Aptura system gives issuers tremendous risk control. They can securely upgrade low-level software using a post-issuance life cycle management system. If a potential security risk or operating issue is discovered, they can download new software or upgrade existing software without conducting a costly card recall.

▶ Personalization Preparation Process

The Datacard® Personalization Preparation Process (P3™), an integrated solution from Thales e-Security, is a software-based system that provides secure key management and data generation for the Smart Card issuance process.

Endorsed by major application providers such as MasterCard and Visa, P3 provides secure key generation, both symmetric and asymmetric, through a hardware security module (HSM) cryptographic resource center. P3 also provides certification generation for card and application certificates, with an optional capability to issue public keys in self-signed formats that are compatible with certificate authorities.

▶ Smart Card Personalization Manager

The management of applications and other Smart Card objects will quickly overwhelm any traditional card issuance operation. To effective manage personalization applications and other objects; you need a centralized, server-based approach that allows you to manage all your card issuance systems from a single point of control.

The Datacard® Smart Card Personalization Manager (SCPM) offers these exact capabilities for Smart Card issuers. This integrated software and hardware platform allows issuers to access Smart Card applications and objects stored in a single, centralized Windows NT™ network server from multiple remote workstations. It helps eliminate the inefficiency and security risks inherent to managing multiple card personalization systems and duplicate applications.

The Datacard SCPM can dramatically increase the productivity, security and convenience of any high-volume Smart Card program-whether supporting one or multiple applications. It is a productive solution credit; debit, stored value, telephony, loyalty and transit applications.

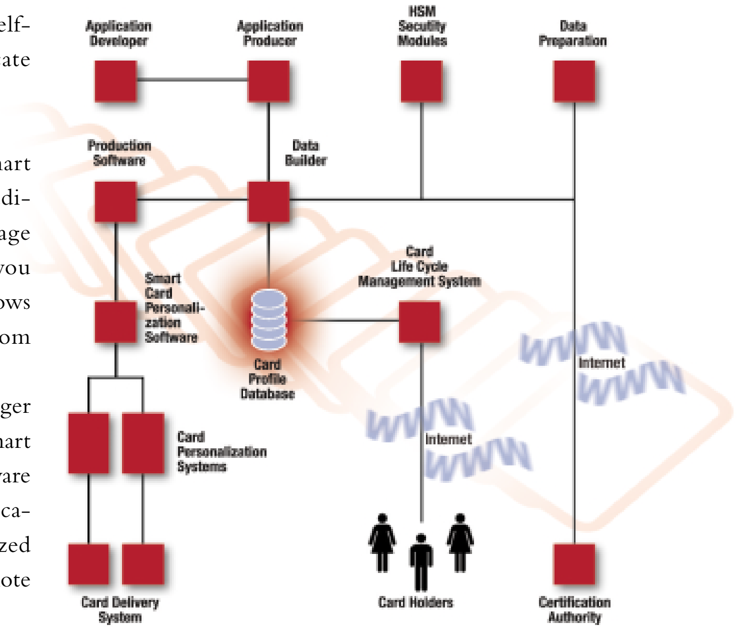
▶ Personalization Applications

Datacard offers Smart Card personalization applications for financial, GSM, e-purse and other common Smart Card applications. These proven software applications, based on MULTOS™ and Open Platform standards, define personalization parameters for specific Smart Card applications.

▶ Card Life Cycle Management

Unlike traditional cards, applications stored on multi-application Smart Card can be changed after the card has been issued. Capitalizing on this dynamic capability requires an ability to add or delete applications securely over the Internet or other private networks. Card issuers will also have to track cardholder and applications data from the time it is issued through the full life of the card. That is why Datacard offers the Datacard® Affina™ Multi-Application Smart Card Management System.

Affina has been specially designed to support secure and productive post-issuance management of multi-application Smart Cards. The system greatly simplifies the management of multi-application Smart Cards throughout their entire service



life. It securely executes the remote loading, changing, blocking, and deleting of applications across a distributed multi-application card base.

Affina also makes it easy to reissue lost Smart Cards with the correct applications and data, and card issuers can generate up-to-date status reports for any individual card. This accurate, real-time information paints a clear profile of the applications held by the cardholder, making Affina a powerful tool for customer relationship management.

▶ **Card Personalization**

Card issuers need to recognize the individuality and preferences of each consumer in order to attract and retain cardholders in a competitive marketplace. The products and services an organization offers to consumers must make them feel unique or they'll simply go elsewhere.

Datacard® gives card issuers the ability to deliver on this concept of one-to-one marketing by offering a complete line of card issuance systems. High-volume systems are design for centralized operations. These proven systems allow card issuers to use photos, graphics, text, embossed characters and other design elements to personalize thousands of cards per hour. Datacard also offers a complete line of desktop systems that are perfect for low-volume or distributed issuance.

Datacard is the world's only solutions provider to offer a complete infrastructure for issuing and managing multi-application Smart Cards.

An expert consultative resource for Smart Card issuers

Whether issuing Smart Cards to consumers, employees, citizens, members students or patients, a card issuer's ability to protect the personal information and financial assets of each cardholder will largely determine the success of its program. Cardholders also need to believe that Smart Cards and applications issued to them will operate reliably.

Most card issuers do not have the in-house skills and expertise required to identify the potential security and reliability issues that will surface as a Smart Card program takes shape. Datacard is uniquely positioned to help them in this area. The company has assembled a team of mathematicians, physicists, cryptographers and Smart Card professionals who fully understand the high security risks inherent to any Smart Card program. This team, called Datacard Consult p7, can quickly uncover unexpected risks and show card issuers how to best guard against them.

Datacard Consult p7 is a premier technical resource for Smart Card issuers concerned about security, reliability and trust. Whether they are looking for chip security analysis, card failure analysis, card evaluation services or software application development, Datacard Consult p7 has the expertise to meet their requirements. These capabilities make Datacard the preferred business partner for leading card issuers around the world.

Quality card integration solutions

Datacard's Smart Card integration Group works with financial institutions, corporations, government agencies, service bureaus and other organizations on a global basis to improve the productivity, effectiveness and profitability of their card programs.

The group has repeatedly proven its expertise in the design, piloting, integration and maintenance of successful card programs everywhere.

▶ **Smart Card programs.** Datacard helps financial institutions, government agencies, transit organizations, telecommunications companies, healthcare providers and schools seize full potential of Smart Card technology.

▶ **Card issuance programs.** The company works with financial institutions, government agencies, service bureaus and other large card issuers to increase productivity and profitability of their operations. It also has proven expertise in converting conventional card issuance operations into Smart Card operations.

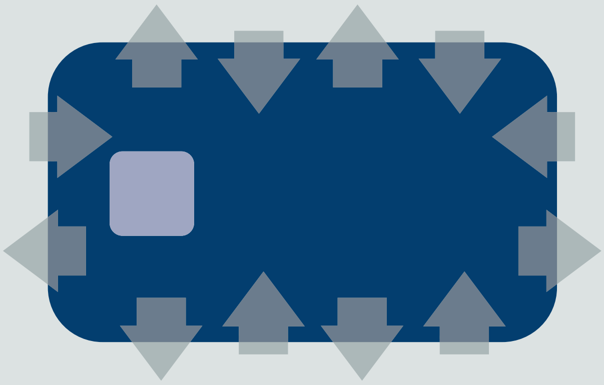
▶ **Identity programs.** Government agencies, corporations, colleges and universities trust Datacard to register identities, build identity databases and develop enterprise-wide identity systems. Successful engagements include national ID, voter ID, healthcare, passport, corporate ID and student ID programs.

www.datacard.com

DatacardGroup

Enabling the Smart Card to Succeed:

An Open Operating System



Within the European market, Germany is a major driving force, especially in the segments for phone cards, SIM cards and banking cards. The phone card segment is characterized by a stable demand with replacement becoming more important as the market changes from intensified development to intensified retainments. Replacement is expected to grow to 1.5 billion cards by the end of 2004. The GSM segment is still growing, although not as strong as in the last years. However, new technologies such as GPRS and UMTS make the development of advanced SIM cards necessary, which will push the market. The banking segment is growing strongly but is restrained by the lack of common standards and interoperability of the operating systems.

The Smart Card market with an annual growth rate of almost 40 percent, belongs to one of the most dynamic high-tech markets in the world. Frost & Sullivan expect Europe to maintain the lead in terms of both units and revenues up to 2004.

This lack of interoperability is one of the restrictions that the researchers of Datamonitor have identified for the Smart Card market. In addition, the price for Smart Card readers have to decrease further, micro-processor cards with larger memory and a wider range of capabilities have to be developed and security features have to be enhanced in order for the market to grow as projected. So far, operating systems for Smart Cards have been proprietary and because of that, a card could only be used for a single task. Even though the industry is still dominated by proprietary systems, there are a few exceptions already on the market that will be briefly portrayed here with their advantages and disadvantages as seen by Datamonitor:

- **Windows for Smart Cards by Microsoft**

The operating system is based on the Visual Basic language and is backed by a large developer community. This leverages the opportunity to reduce time-to-market for new applications. Windows 2000 has built-in Smart Card security tokens and guarantees interoperability with the Microsoft product family, which no doubt makes it a good alternative for PC-based Smart Card use in both the B2B and B2C segments. Costs for the operating system are low, however, and since its launch, deployment of Smart Card for Windows has been very limited. Because of that, the company announced that there would be no further updates of the operating system. However, Microsoft has announced that it is licensing the source code (operating system plus development tools) to major customers and technology providers.

- **MultOS by the Maosco Consortium**

MultOS is designed with a strong emphasis on financial services suitability and its high security specifications reinforce this. MultOS' programming language is Mel, not a widespread language in developer circles, and it is an expensive system option for card-issuers. A C++ compiler is available, but not used very much as it needs a lot of memory space on the chip. Maosco is working together with GlobalPlatform on a single technical approach for issuers who need to manage multiple application Smart Cards, regardless of the card-operating platform.

- **Java Card by Sun Microsystems**

The great advantage of Java is its ability to function on its own as an operating system at the same time as it can overlay other operating systems and run on top of them. Java cards are roughly 20 percent more expensive than proprietary alternatives and require large amounts of memory. Security is also an issue where competing systems have an advantage.

As you can see, the existing non-proprietary operating systems nevertheless have some restrictions: either in security features, cost or because they are tied-in to certain applications. Their main weakness however, is the fact that each runs only with the chip of a certain semiconductor manufacturer.

Total interoperability for no cost

The ongoing domination of the market by proprietary operating systems is especially difficult for the German market, where a lot of independent card manufacturers are operating. They do not have their own operating systems and do not want to buy them from their competitors. The Danish company Logos Smart Card A/S, a subsidiary of ACG AG, solved that problem by developing an operating system that is totally independent of any semiconductor manufacturer as well as any card manufacturer, available across all hardware platforms and free of charge when sold as API (Application Programming Interface) – flashCOS.

flashCOS is a Smart Card operating system, that can be used for almost any purpose. The operating system is based on the widely used programming language C. Any application specific software written in C can be loaded onto flashCOS. Thereby the function of the operating system can be extended and new interface commands can be added. It is also possible to override existing commands and give them another function. In this way, flashCOS can be customized to implement the requirements of almost any existing Smart Card application.

The core of this concept is fully realized software modularity. The two main modules are the hardware abstraction layer (HAL), and a full implementation of the ISO 7816-4 command set, that is able to work on ROM as well as on flash hardware. Therefore, flashCOS is available as a flash and a ROM version. The advantage of flash over ROM technology is that it increases the hardware efficiency. A 16kB product offers a 32kB function. Regarding the security aspect, flashCOS offers a command and response encryption, a secure file system and DES, 3DES, MD2, RSA and ECC security function libraries. The files in the file system on flashCOS can only be read, written or otherwise manipulated, providing the card reader and user have acquired precisely defined access rights. This prevents unauthorized access to files on the card.

The completely modular set-up of flashCOS, based on open standards, guarantees short development times and enables the development of applications via compiler directly on the PC and without detailed knowledge of the hardware. Customers can even exchange and enhance applications over the Internet. Under www.flashcos.com an information center is available, which is intended to become a focal point for all customers. flashCOS can be used as a single-function or multi-application card. In the first instance it is, however, a single-issuer card in the sense that a single authority has total control of the card.

Product derivatives for special purposes

Several derived products were developed off flashCOS. flashCOS GSM was tailored especially for the largest micro controller market, mobile telephony. The product range covers the low-end phase II market as well as high end markets with PKI requirements. The product range goes from small memories up to a 128kB EEPROM chip. It also supports dual and triple mode phones (CDMA, TDMA, AMPS). flashCOS GSM is available with a variety of standard applications: an API programming interface, a scripting and byte code interpreter (LSCript) that makes the writing of applications easier and faster, a Wireless Internet Browser (WIB), or a user localizing interface.

A Java version is being developed for Smart Cards that can be partly managed by several independent authorities each not having access to each other’s program and data on the card. The Java version will be equipped with a firewall and comes as a full version and a SIM derivative. It will be available in the first quarter 2002.

This article was first published in Card Forum International, issue no. 7/8, 2001

Securing Interests Through Secure Licensing

By Sospita ASA

The reality today is that even with substantial revenues and a healthy yearly growth rate, at least $12 billion worth of software is pirated each year. As a result, the legitimate owners of intellectual property are suffering immense losses. With license keys being cracked every day, illegal software copies flourish. Since producing software is expensive and time consuming, the need to secure this investment is clear.

A major goal today is to protect intellectual property owners from losses associated with software piracy, by offering cost-effective and flexible licensing solutions with a level of security, where the cost of breaking the protection exceeds the benefit.

As software developers invest fortunes to develop their software, and with new distribution models emerging, more and more companies are feeling the need to insure against piracy.

The common and risky way to unlock protected software is by giving the software's license key to a person you hope you can trust. Once he has opened the "safe" and executes the application, the software appears as clear text in the computer's memory. Consequently, these "trusted" people would have access to all the information needed to crack the application and give it away or sell it for their own profit.

What is needed is a solution that allows software developers the ease of encrypting portions of their code. Once the code is functional, using an SDK, such as the Sospita Development Kit, developers can select valuable parts of their code and protect these parts using strong encryption. (See figure 1). After doing so, the source code can be compiled into an executable program using a standard compiler.

Preventing decrypted code from appearing in clear text in the PC's memory is the core of Sospita's technology. Sospita License Protection enables the encryption of parts of the source code during software development, and establishes a corresponding license key.

After protecting a software application using Sospita License Protection and assuming the end-user has paid for a valid license key, at runtime the protected code is actually moved away from the computer to a secure environment, namely a USB token or a Smart Card. Using the built-in processor in the token or the card, the protected software code is decrypted and actually executed on the token without any trace of execution left on the host computer for prying eyes. (See figure 2).

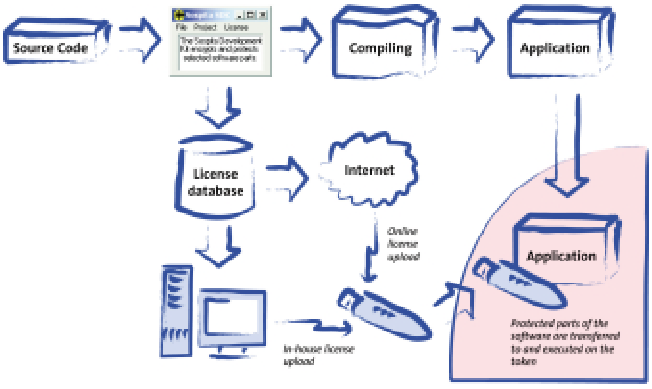

Source Code
File Project License
The Sospita Development Kit encrypts and protects selected software parts
Compiling
Application
License database
Internet
Online license upload
In-house license upload
Application
Protected parts of the software are transferred to and executed on the token

Figure 1 - In the development phase, software vendors use the Sospita Development Kit to protect selected parts of their application. The SDK allows the developer to chose which parts to protect. These parts are encrypted using the development kit's precompiler. Once this is done, the source code is ready for compiling by an ordinary compiler such as Microsoft Visual C++™. The finished application will appear as a combination of clear-text and encrypted code.
In the runtime phase, the end user will need a way of decrypting the encrypted code. By using the Sospita Secure Token, the encrypted code is moved from the host computer to the token where it is decrypted and actually executed. Without a token containing a valid license (decryption key), the software simply will not run. This is the core of the Sospita License Protection technology – executing parts of the application in a tamper proof environment, such as a Smart Card or a USB token.

The patented Sospita License Protection technology consists of several modules. The modules communicate tightly with each other, providing a highly secure and reliable software protection solution, based on open standards and state of the art technology.

The Sospita Development Kit allows developers to protect software easily and with a high degree of security. The software application can be written and debugged using an ordinary compiler and debugging tool, then the code sections are simply marked for encryption and the development kit protects it. The application then interacts with the Sospita Runtime System, which provides the interface between the license protected software application and an external token. Moreover, the Sospita Runtime System is installed with the protected software, and is therefore transparent to the end user. The Sospita Secure Token is a high performance, tamper-proof hardware token with a main processor (CPU), crypto co-processor and memory. The token controls all security pertinent operations, and executes the protected parts of the software application. Tokens are available as Smart Cards or USB tokens running on Windows for Smart Cards, Java card, or Sospita's highly optimized native operating system QX. These cards can be company branded.

For those applications where the end-user base would not accept a separate tamper-proof device, the Sospita Software Token fully emulates the hardware token, allowing a software token to replace a hardware token. Although the software token does not provide the tamper-proof security furnished by hardware tokens.

There are two different solutions for managing both small and large-scale distribution requirements, which both allow token firmware upgrades. Sospita License Manager handles small to medium scale needs. Functionality includes secured services, such as maintenance, token status monitoring (licenses and permissions available), and license downloading from a license server, license backup, license moving, and license deletion. Software developers can generate new licenses and copy these to new tokens to be distributed to the end-user. Sospita License Manager Pro offers additional license management functions, such as authentication, secure download of licenses, license usage metering, and license inventory and license revocation via the Internet or over an intranet. Also, different payment solutions can be integrated with the license manager.

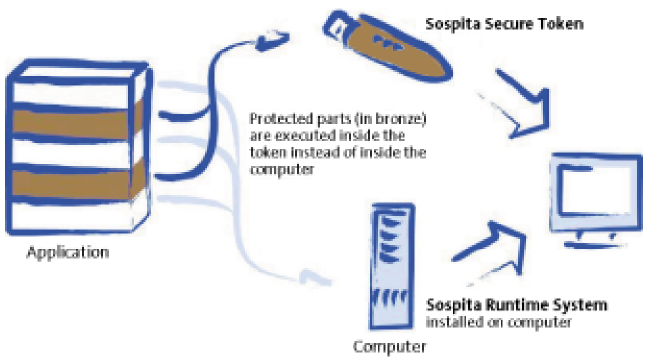

Sospita Secure Token
Protected parts (in bronze) are executed inside the token instead of inside the computer
Application
Sospita Runtime System installed on computer
Computer

Figure 2 - Execution of encrypted software on token - the patented technology from Sospita

This patented technology opens a completely new range of opportunities for the software industry. It is now possible for 'peace of mind' distribution of software over the Internet, with full control of licenses. A number of flexible revenue models can be realized. For instance, demo software can actually be full source code that is feature protected, or basic functionality offered at a low price can be upgraded with a simple e-commerce transaction. This also encourages viral distribution, since Sospita's solution is based on usage protection and not merely copy protection. Furthermore, the solution provides the opportunity to offer a client-side rental license program for either a predefined period or actual usage period with full vendor or service provider control, such as pay-per-use and try-before-you-buy. In addition, the solution is designed with the end-user in mind, as the token has the ability to store multiple vendor-independent licenses where companies can benefit from joint marketing opportunities.

With the growing adoption of Smart Card technology worldwide, both vendors and end-users will be looking for multi-application solutions that provide added value and a higher level of protection than currently in use.

This article first appeared
in Card Forum International
May/June 2001 Volume 5
Number 3.

sospita
Protecting Your Software

www.sospita.com

Running Commentary

Calum Bunney

The security business is designed to confuse. Sometimes it succeeds in confusing most of us, at which point of course I turn my eyes to the sky and say "well thank goodness for the Silicon Trust, beating a path through the long grass with a long stick". From time to time some security issues become clearer and, having read through this issue, I'm convinced that the castle moat is now filled with deep water and sharp-toothed fish, and that the chains pulling up the drawbridge are well oiled.

As discussion of random number generation and the suppression of unwanted noise takes over the domestic affairs of castle life, then clearly our basic ideas about security are changing. In the Pyrenees of Southwest France the Cathar castles built in the C12th were thought to be impregnable, high up on the cliff tops. When it came to attack you either sat inside eating sandwiches waiting for your attackers to go home (denial of service), or jumped off the walls, or stepped out the one front door with your hands up (sold your stock and trusted in the free market). By contrast the invasion in October 1917 of the Czar's Winter Palace in Russia (not really a fortress) was a hopelessly unsuccessful affair, where many of the intended captives quietly made their escape through the hundreds of doors, windows, and corridors available. Stealth and complexity matter.

While those who like to talk security before breakfast are already advocating intelligent monitoring within systems, and even security counter-attacks (let's not discuss here the possible legal argument over who took the first byte), most members of the public only really seem to understand the locked box approach to security. When it comes to security we tend either to keep it under the mattress or we follow tradition and do what most other people do without asking questions, we go to a bank. The observation in these pages that the mobile phone (GSM of course) is the Volkswagen Beetle of the Smart Card industry is particularly telling. High tech rolled into low telecom. The public may talk another language but it is still possible to find a way for the two cultures to coexist. Christ after all rode a mule not a Maserati.

Perceptions do change, and not always slowly. Who would have expected that ten years ago we might all be fascinated to watch the dirt being sucked off our carpets into a transparent vacuum cleaner. Greater public interest in being clean has opened up the technology as much to public interest as to scrutiny. How this will translate for security issues is harder to say, but better selling of the process might have a role to play. Confidence in virus checking software is improved for example by the user interfaces: like the dirt in the vacuum cleaner, we can see the little bugs being swept away: a roll call of nasties.

Security needs a face. For banks the ATM is one face of security: with a card slot reassuringly like that of a tight-lipped bank manager. If we are talking about the public at large then we are perhaps not really dealing with tokens as we understand them technically, but with icons, symbols of security and reassurance. Is it the smart chip on the bankcard that means security to the bank's customer, or is it the name Dresdner Bank? We know the two to be joined (the bank chose the card) but they may seem unconnected. If we were to offer a simple magnetic stripe card with the bank's name onboard, and a Smart Card with a quite well-known company name on board (let's say Infineon) then I'm willing to bet that the inferior card wins most times with the public.

The USB familiarisation issue raised in these pages also argues that there is a gap to cross between technologies that are perceived as family members or as household guests. For a little reassurance here we might look next to what will happen with USB fingerprint readers as these seem to offer a real chance of merging plug and play friendliness with the friendly face of security.