

s@ecure

www.silicon-trust.com The Silicon Trust Report

WH  ARE YOU? WHO ARE YOU?



Read about
Silicon based
Security Solutions:

- Biometrics**
- Smart Cards**
- Embedded Security**
- ID Systems**

Who are you? Can I trust you?

These questions are the basis of any relationship we have with each other.

Our daily lives are influenced by the degree of trust that surrounds us and the sense of security that comes from it. The events of September 11 have been a test of that sense of security. The realization that the biggest threat comes

from within, unidentified and right in the middle of our safety zone, puts a strain on the concept of trust. Thus we have witnessed a revival of discussions on nations ID cards, as well as the implementation of

other ID projects. The technologies at the heart of these projects are Smart Cards, biometrics or a combination of



both. In this issue of Secure we want to illustrate the complexity of such Identification systems.

Generally speaking, we believe that Smart Card technology can help protect privacy. Personal data can be stored decentralized on a tamper-resistant personal token, allowing the user to be more in control of his/her own data than if it was stored on a central server or on central paper files. Biometrics enables the authentication of a user, limiting the abuse of personal data even further.

While the discussions continue, we are working on making sure that the technology becomes safer, easier to integrate and tailored to the requirements of each application. For example the Infineon 88 Family of Smart Card Controllers: it comes with plenty of memory headroom, as well as the most advanced security concept on the market

to cater for the most sophisticated projects. Find out more in Bernd Meier's article, starting page 32.

As we are using this issue to ask questions such as "Who are you" and "Can I trust you", we felt that we should cast an eye, (no pun intended!) over the market segment that is currently called "Identification".

You can read Marcel Hametner's article on page 26 as he brings a focus upon business models currently being satisfied by silicon-based solutions available for the ID-market.

For frequent updates on what is going on in the world of Smart Cards, RFID, dongles and biometrics, don't forget to bookmark www.silicon-trust.com.

Veronica von Preysing

Impressum

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

SECURE - The Silicon Trust 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
Cover Stefan Gassner © 2002

Advertising & Distribution

Karen Brindley
Email - karen.brindley@krowne.de

Printing

ADM Bozen
Siebeneich-Terlan, Italy

This issue of SECURE - The Silicon Trust Report is Copyright 2002 by Infineon Technologies AG.

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

No portion of this publication may be reproduced in part or in whole without the express permission, in writing, from the publisher. All product copyrights and trademarks are the property of their respective owners. All product names, specifications, prices and other information are correct at the time of going to press but are subject to change without notice. The publisher takes no responsibility for false or misleading information or omissions. Any comments may be addressed to the Silicon Trust Program Director - Veronica Preysing (veronica.preysing@infineon.com)



6 Contributors

Who's who
in this Issue

8 Highlights

What's new at
Infineon Technologies

10 Introducing the Silicon Trust

11 Welcome to the Trust

12 Info-Box

Smart Card and Biometric
Industry News Exclusively
from Ctt and Btt

14 Industry Initiatives

The Evolution of the Trusted PC

In today's society we take for granted the technology of Computers; demanding flexible, advanced software programs plus secure ways of interacting with other Users. But this mix of requirements can sometimes be conflicting, and is not necessarily easy for the PC Manufacturers to achieve. This is why the TCPA (Trusted Computing Platform Alliance) was formed by Compaq, HP, IBM, Intel, and Microsoft; to standardize security and privacy levels across the whole industry, without compromising the sophistication and diversity of software.

18 Working Within TeleTruT

The non-profit organization, TeleTruT was founded in 1989 and has been increasingly active internationally since 1997. The aim of TeleTruT is to support the development and awareness of trusted information and communication technology. To achieve this, applications for trusted, forgery resistant and verifiable electronic business transactions are promoted.

20 Application Focus

Market Trends and Hardware security for banking and brokerage applications

After the unprecedented hype for e-business transactions, the online world is changing once again. The first online business models focussed on the winning of online users. Access fees for online providing services and secondly web advertising with a correspondent click rate promised financial success. But the use of these business models meant that only in very few cases was money actually made.



20 Application Focus

Market Trends and Hardware
security for banking and
brokerage applications



26 Application Focus

It's all about Identification ...



32 Technology Update SMART CARDS

Multi-Application Card
Controllers Go 32-Bit



36 Open. Independent. Free. flashCOS® sets New Standard for Smart Card Operating System

26 It's all about Identification ...

"Identification" as market segment is reported to have the largest smart card segment potential, which is something that Infineon Technologies takes very seriously as it means an enormous revenue return over the long term. Being responsible for our approach towards this market segment, I was asked to write about "Identification". The article was to include a quick overview of what the segment is all about and describe briefly how this segment will change over the next few years.

However, if I were to go into depth on any one of these markets, I could spend the entire article on it (similar to an article on banking, GSM or transport). This approach, unfortunately, would not bring the reader much in terms of the whole segment itself. Instead, I will try to do justice to the article by outlining the complete segment itself, the market, and some of the technologies out there. Primarily, I will focus upon business models being satisfied by silicon-based solutions for the ID Market.

32 Technology Update SMART CARDS

Multi-Application Card Controllers Go 32 Bit

Today Smart Cards can be found in GSM SIM cards and banking cards, although the functionality is very specific and the number of applications per card is very limited. Any mainstream hardware out in the market tends to be based on 8-bit controllers with memory configurations of up to 32 kByte of E2PROM, 136 kByte of ROM and 6 kByte of RAM.

However, the evolution of the Smart Card is currently going in a new direction. The major trends in the market for Smart Cards are for those cards with enhanced services, with the capability of executing multi-applications on a single card. Additionally, the issuer of the card wants to offer the possibility of downloading new applications and functionality to the card - in the field. The software implementation available today is based mainly on a proprietary operating system with embedded applications. Together with the trend for multi-applications, the market is starting to demand open platform systems, based on virtual languages, like Java SCTM. The idea behind this is to separate the operating system and the application software in a standardized way, which will finally allow different parties to write applications for various numbers of services.

36 Open. Independent. Free. flashCOS® sets New Standard for Smart Card Operating System

Leading market researchers currently expect a great future for the Smart Card and indeed, the figures seem to back that analysis. With an annual growth rate of almost 40 percent the Smart Card market could be considered one of the most dynamic high-tech markets worldwide.

Another growth market – albeit in a more moderate way – will be the SIM-card segment for mobile communication. Datamonitor expects the microprocessor card, which is the central part of a mobile phone, to grow by 21 percent until 2006.

40 Power and Timing Analysis Attacks against Security Controllers

The methodology of power analysis is based on a simple effect (also found in other disciplines such as physics and medicine). Namely, that wherever electrical currents appear, the flow of electrons can be detected, directly or indirectly, in its vicinity.

46 Technology Update BIOMETRICS

Biometric System Security

The availability of the biometric application programming interface, Bio-API, has facilitated the integration of biometric systems into applications. One of the important considerations in the definition of the API was to identify and prevent any potential security attacks that could arise as a result of its usage. This article describes how a particular attack, known as the “hill-climbing” attack, was identified and resolved during the development of BioAPI.

50 Improving Biometrics

We are frequently seeing biometrics proposed as solutions to identification problems in commercial and government applications – especially those associated with international border control and welfare payments. In the UK alone financial losses in this latter area due to mistaken identity are believed to be measured in billions of pounds annually. Unlike its PIN and ATM card counterparts, a biometric has the advantage of being non-transferable. But in the past the use of biometrics has been stymied by the demands of the technologies involved, cost and large, variable user populations. It is partly for this reason that deployment of biometrics has been patchy. This is now changing. Recent progress in biometrics suggests that performance accuracy can be improved in a number of ways. We consider how.



40 Power and Timing Analysis Attacks against Security Controllers



46 Technology Update BIOMETRICS

Biometric System Security



50 Improving Biometrics



56 Biometric Identification and National Security

56 Biometric Identification and National Security

Since September 11th 2001, innovative technologies have been seen as a way to heighten national security.

58 Security Is Just a Fingerprint Away

In today's ever-changing world of information technology, securing critical information and data continues to emerge as the number one concern for all IT managers.

Passwords secure information, but not as securely as IT managers need. Most liken password security to a necessary evil, but few neither believe in the security nor want to manage a password-based security system.

60 Technology Update EMBEDDED SECURITY

Infineon's TPCA-compliant security solution supports all PC security applications

Communication over the Internet is growing continuously. Many applications, such as those intended for eCommerce, are based on trust in the communication partner and the reliability of the connection.

61 Within the Trust

The CardMan Fingerprint 7120 from OMNIKEY

Smart Cards are increasingly being used for applications such as Payments, Home-Banking, Smart Card based Authentication (SingleSignOn), Digital Signature Internet-Security, e-commerce, PKI-Tokens, Health cards, Loyalty etc. At the same time, biometric technology is needed for a more secure and convenient access to Smart Cards and applications. OMNIKEY's CardMan® fingerprint product-family facilitates the use of Smart Cards in combination with biometrics.

62 Taking care of your business advantages from Sospita

Ever heard of software reverse engineering? Want to know how you can protect your software from being reverse engineered?

64 Apollo-CL: The Multi- Application Smart Card OS from SC²

The Apollo CL is a natural choice for many applications, including public transport, toll collection or access control as well as for many IT applications, offering easy access to contactless memory through any Type A or Type B reader.

66 Running Commentary by Calum Bunney

Who's Who

IN THIS ISSUE?

► Henning Arendt

Henning Arendt has a consultancy company: @bc® – Arendt Business Consulting and is a Business Consultant for Financial Service Providers and Trustcenter Services. He is an EU expert for biometrics and a speaker at international conferences.



Henning is the Project manager for BioTrusT/TeleTrusT Deutschland e.V., a member of TeleTrusT Deutschland e.V. and European Electronic Messaging Association (EEMA) and a member of the board of Frankfurter Finanz Forum e.V. He has had 25 years with IBM, 5 years based in the U.S.A., covering various management and staff assignments: marketing manager, account executive, international product manager. His University degree (Dipl.-Ing.) is from the Technische Universitaet Hannover.

► Monika Bremer

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)

► 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.

► Marcel Hametner

Being born and raised in South Africa and attained an Electronic Engineering degree, Marcel Hametner started his career as a hardware & software design engineer at Siemens Ltd., South Africa. He was appointed regional manager for Security & Chip Card ICs in November 1997. As business executive he was responsible for both the regional market development and account management. In June 2001, Marcel



Hametner left Siemens and moved to Munich, Germany. There he joined Infineon Technologies (Security & Chip Card IC Division) as Director of New Markets & Relations, heading up the Identification segment. This position includes market segment understanding & development. His main focus areas are to create & evaluate new business opportunities, define business models and build a comprehensive relationship network in this field.

► Olaf Jacobi

Olaf Jacobi is Head of ACG's Smart Card Group and has been a member of the Board of Directors since August 1999. Before joining ACG, he held several positions at Minolta. Olaf Jacobi studied Economics at the University of Hamburg.



► Marcus Janke

Since 1991 Marcus Janke has been working on the conception, development and realization of Stand-alone and PC-based Smart Card terminals. Since 1993, as an author and columnist, he published numerous publications covering the sectors of Smart Card technology, applications and security concerns and held



several lectures in this field at international conferences. Marcus carried out consultancy work for television companies such as ARD and ZDF as well as for print media. After his diploma thesis in electrical engineering at the university of Hamburg 1997, including the development of a dedicated PC Smart Card terminal system, he started working with NEWTEC-Ebert GmbH in Hamburg directing the unit for Smart Card applications.

In September 1999 he came to Infineon Technologies AG, Munich, where he currently manages the security concepts sector for Smart Card product security, expanding his focus on the system and application security.

► Dr. Peter Laackmann

Dr. Peter Laackmann has been developing hardware and software components



for synchronous and asynchronous Chip Card terminals since 1991.

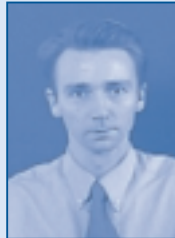
He has written both technical articles and columns for numerous publications covering Chip Card technology, applications and security concerns, and between 1993 and 1999 also carried out consultancy work with television companies such as ARD, ZDF, SAT1, Pro7.

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 Kuratorium Deutsche Kartenwirtschaft – going on to complete his PhD at the Christian Albrechts Universität in Kiel.

He currently manages the Product and System Security department (Security and Chip Card ICs) at Infineon Technologies AG in Munich Germany.

► Bernd Meier

Bernd studied Electrical Engineering at the University of Bremen (degree Dipl.-Ing.)



After three years of working as a Field Applications Engineer for a US semiconductor company, Bernd Meier joined Infineon Technologies in 1999 as Product Marketing

Manager within the business group Wired Communications. Since 2001, he holds the position of Marketing Director for 32-Bit Chip Card Controllers within the Chip Card IC business unit.

He is responsible for the worldwide marketing and the product definition of Infineon's 32-Bit Chip Card Controllers.

► Keith O'Leary

Keith O'Leary is a seasoned technology professional having worked in the software industry for over



15 years. He has held senior roles in both product management and product marketing for companies such as Lotus Development Corporation,

IBM and Netegrity. He is currently directing the product and marketing activities for Keyware's core software product suite of Central Authentication products.

► Dr. Colin Soutar

Dr. Colin Soutar joined Bioscrypt Inc. in 1994 and currently holds the title of CTO and VP, Research and Development. Colin is responsible for Bioscrypt's advanced technology projects and corporate technology strategy. Colin also



represents Bioscrypt on the Steering Committee for BioAPI, the biometrics industry standards, for which he is currently Chair of the Reference Implementation Work-

group. Prior to joining Bioscrypt, he worked on optical correlation systems at NASA Johnson Space Center in Houston, Texas. Colin received his Ph.D. in physics from Dundee Institute of Technology in Scotland in 1992. Colin is the author of many scientific publications and several patents.

► Dr Susan Thompson

Susan is the chief security mathematician for Datacard Consult p7 with 17



years experience in security and cryptography. Relevant experience includes:

Design of secure cryptographic algorithms used for recent major projects, with particular emphasis on public key cryptography;

Awareness of microchip cryptographic capabilities and study of future chip design; Signal and power analysis of smart card chips; Investigations into future algorithms, including elliptic curve cryptosystems; Design of new biometric systems; Design of methodologies for Smart Card evaluation, including Common Criteria and ITSEC; and Monitoring of the global security and cryptography scene, including attendance and involvement with the organization of crypto conferences. Previously, as head of the System Security Group at Plessey Crypto, she worked on a number of technical assignments involving broadband/narrowband speech encryption in mobile/static environments, data/fax encryption and secure packet switching networks. She was also involved with the EFTPoS UK project producing design specifications for security components and security procedures.

Infineon Technologies and Sony to Cooperate on Contactless Chip Card ICs

Infineon Technologies and Sony Corporation announced on the 13th November 2001 that they will jointly develop secure integrated circuits (ICs) for contactless Chip Card systems. Combining Sony's contactless Chip Card



technology "FeliCa", which is based on Type C, and Infineon's expertise in secure Chip Card ICs, the agreement will expand the contactless Chip Card market including multi-application cards, card terminals and background

infrastructure systems for data management. The jointly developed ICs are targeted to be available by the end of 2002. These ICs will be integrated as dual interface chips that have both contact and contactless interfaces.

The cards combine authentication and identification with the stringent requirements for fast authorization in access applications, such as electronic tickets in public transport, company or government issued ID cards, and banking cards. Based on their encryption and decryption functionality, the cards enable secure and reliable transactions.

"Market success of contactless chip card applications depends on the ability to provide complete solutions. Combining Sony's system know-how with Infineon's expertise in secure semiconductor solutions and manufacturing processes will provide the benchmark for contactless technology of the future," said Dr. Hermann Eul, senior vice president and general manager of the Security & Chip Card ICs Business Group of Infineon Technologies. "This agreement enables complete system solutions paving

the way for powerful Chip Cards that combine multiple applications such as public transportation services, electronic purse systems and identification, as well as best-price loyalty programs."

"I am delighted that Sony and Infineon have reached this agreement to jointly develop chips, which introduce Sony's Type C contactless Chip Card technology. Our cooperation will result in the application of this technology in transport systems, as well as in the finance and administrative fields. We also plan to offer many new access-modes for Sony's FeliCa as a key network device technology for the future," said Hiromasa Ohtsuka, President of Sony's Broadband Network Center.

The agreement combines Sony's expertise in contactless Chip Card technology with Infineon's know-how in design of secure Chip Card ICs and state-of-the-art manufacturing processes. Under the terms of the agreement, Sony will contribute its Type C contactless Chip Card specifications and FeliCa operating system. Infineon will integrate this interface technology in its contactless IC product family. Infineon will manufacture the dual interface ICs with the jointly defined Type C secure technology and supply them to Sony.

New Secure Microcontroller from Infineon Technologies Receives Prestigious "Sesames Award"

On October 29, 2001, Infineon Technologies announced that its new 32-bit Chip Card controller was named as Best Technological Innovation 2001 and recipient of a Sesames Award. The award was announced during "Cartes 2001" in Paris, France (October 23 - 25, 2001).

The Sesames Awards, now in their sixth year, honor outstanding achievements

within the Chip Card industry. An international panel of nine jurors active in the Chip Card industry selected the individual recipients from a total of 86 companies that applied for the nine Sesames Awards, which recognize the winners in the categories "Best Application", "Best Software" and "Best Technological Innovation".

Infineon received the award for the first member in the new 88 family, the SLE88CX720P. Featuring unsurpassed computing power and leading-edge security capability, the chip sets a new standard in performance and flexibility in the Chip Card category.

The SLE88CX720P supports secure and reliable administration of several applications on a card. It will accelerate the

evolution of chip-on-card products into multi-functional Chip Cards, combining features such as an authenticated driving license with banking and credit card services, monthly ticket for public transportation, and the loyalty bonus program of a retailer.

"Our new 32-bit Chip Card controller has been well received by our customers due to its forward-thinking product features," said Dr. Hermann Eul, senior vice president and general manager of the Security & Chip Card ICs Business Group of Infineon Technologies. "The award strengthens our trust that our 32-bit Chip Card platform, the 88 family, will become the most successful of its generation - just like the 66Plus and 44 product families in the past."

Infineon Technologies Provides Secure Microcontroller Chip Used In U.S. Department of Defense Smart Card Program

Infineon Technologies has announced that it is supplying secure microcontroller chips used in Smart Cards now being issued by the U.S. Department of Defense (DoD). The Infineon chip is a component of the only currently available Smart Card that meets the stringent requirements specified by DoD, including FIPS 140-1 Level 2 Certification by the National Institute of Standards and Technology (NIST). The

DoD Common Access Card (CAC) is being rolled out as the single standard means of physical identification, building access and computer network access for approximately four million civilian and military employees and outside contractors.

Infineon manufactures the secure microcontroller used by SchlumbergerSema in the Smart Cards provided to the DoD by Electronic Data Systems Corporation (EDS) under a contract awarded as part of the Defense Manpower Data Center's Common Access Card (CAC) program.

In Smart Cards like those used in the CAC program, the secure microcontroller works like the processor of a personal computer to run the operating system and application software. The microcontroller has advanced security

capabilities built-in, such as support for Public Key Infrastructure (PKI) and digital signature technology. These features work with other elements on the Smart Card to protect stored data and to ensure that only the individual owner of a card is able to use its features. In addition to the microcontroller, the card contains a magnetic stripe, a linear bar code, a 2D bar code, a photograph, and several anti-counterfeit security features.

The CAC program specifies Smart Card technology that is based on the open-Java platform and meets the stringent requirements of Federal Information Processing Standards (FIPS) 140-1 Level 2 certification. This provides both high-level security capability and the flexibility for the DoD to add additional application programs to the Smart Card in the future. (*see Secure no. 02/2001*)

Second SECURITY SOLUTIONS FORUM held for Partners of Silicon Trust

Held in Munich from the 20th to the 21st September last year, the 2nd **SECURITY SOLUTIONS FORUM** was open to members of the Silicon Trust. However, this time, there was more than just hardware suppliers represented from the Biometrics arena – there were also software suppliers, integrators and representatives from the Smart Card industry and players within the Embedded Security market.

The partners themselves took the time to train and enlighten other members of the Silicon Trust on their products and solutions, as well as their view of current security markets. Alongside the Technical Tracks, Infineon also hosted some Marketing Round Tables on the subject of E-Business. During these round

tables, time was spent discussing a joint marketing approach to this ever growing market sector resulting in solid action plans and a time table for implementation.

The feedback from the partners was one of satisfaction. Solid results are coming

out of these 2 day forums which the partners can take away and in turn develop real networks and business opportunities from.

An agreement was made for a third **SECURITY SOLUTIONS FORUM** to take place in the second quarter of 2002.



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 products 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**

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 and the Security Solutions Handbook.
- Participation with and assistance from, Infineon Technologies during key industry events.
- Use of the Silicon Trust Logo for your promotional material.

Technical Benefits

- Free participation at the Silicon Trust Security Solutions Forum
- Discounts on training courses for your developers.
- Access to Infineon Technologies' top application engineers.

Members of the Silicon Trust

- ACG
- Aladdin
- Association for Biometrics
- Bioscrypt
- CE-Infosys
- Datacard
- Faktum
- G&D
- Guardeon
- ISL
- Loqware
- Omnikey
- Pollex
- Precise
- PSE
- SC²
- Secartis
- Siemens
- Sospita
- Teletrust
- Towitoko

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.

Welcome to the Trust

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

Guardeonic Solutions AG

Guardeonic Solutions AG offers IT-security system and consulting services to international customers in the banking and financial services, logistics and health care industry.

As an Infineon Technologies AG company Guardeon integrates leading product developers and solution providers including e-payment, PKI, cryptology and IT-technology expertise into a new business group.

www.guardeonic.com



Teletrust

Teletrust is a non-profit-making-organization for the Promotion of Trusted Information and Communication Technology.

Major tasks are in applied cryptography and biometrics. Teletrust's 119 members come from research, development and politics and essential fields of application. It builds upon the collaboration of the most varied producers of security solutions. Since 1989 Teletrust Germany is active as a non-profit-making-organisation – politically and economically independent.

Teletrust in an Affiliate Member of the Silicon Trust.

www.teletrust.de



Association for Biometrics

The Association for Biometrics is an organization based in the UK, set up with the following objectives:

- Development and provision of various resources to support the Biometrics community eg: information database
- Organizing meetings, forum, short courses and workshops.
- Sponsoring and supporting conferences and exhibitions.
- Development and promotion of standards.
- Development and promotion of best practices in Specification of Requirements and Evaluation.
- Building awareness of Biometrics technologies and applications through active educational programs.
- Positioning of Biometrics within Information Communication Technologies (ICT) courses and curriculum planning strategies.
- Establishing and maintaining links with appropriate organizations.
- Identifying research opportunities and promoting collaborative research.
- Active liaison with appropriate national and international Government Agencies.
- Encourage informed debate on non-technical issues arising from the deployment of Biometrics, such as privacy and public acceptance.

Association for Biometrics is an Affiliate Member of the Silicon Trust.

www.afb.org.uk



A date for your Diary!

9, 10 April 2002 Brussels, Belgium, Biometrics:

Business & Security 2002

This event, the first of its kind, will focus in-depth on three of the hottest application areas in the biometrics industry today – the law and order, financial services and travel industry sectors. In addition, a separate stream of speakers will address the wider issues facing the industry, together with an update on all the cutting edge technological developments.

To get more information on how to attend this year's conference, see our ad in this issue or visit

www.biometricseurope2002.com

ERG buys Proton World

Ctt November 2001

ERG Group of Australia has bought out its partners in Belgian-based Proton World International (Proton World). To pay for the acquisition, ERG is issuing the former shareholders of Proton World – American Express, Banksys (Belgian banks), Interpay Nederland (Dutch banks) and Visa International – with approximately 75.5 million shares (representing 8.4% of ERG's capital). In addition, ERG has agreed to pay some A\$58.8 million in cash. The agreements with American Express and Visa International also provide entitlements to options on ERG shares.

The sale agreements call for long-term (5-7 year) service level agreements to be executed by American Express, Banksys and Interpay Nederland. The contracts are expected to generate revenue in excess of A\$200 million.

Proton World was formed in 1998 as a joint venture between ERG, Banksys, American Express, Interpay Nederland, and Visa International. There are now

more than 35 million Proton-based Smart Cards in circulation and more than 500 banks have deployed the technology.

GSM card deliveries back on track despite September 11

Ctt November 2001

Recent forecasts for total deliveries of (high value) GSM cards for 2001 ranged from 320 million units (Gemplus) to over 400 million (Schlumberger). A panel of the industry's senior executives, meeting to comment on the latest figures from Eurosmart, made the estimates.

The prevailing opinion was that the pre-Christmas rush in 2000 to shift cell phones was not going to be repeated in 2001, but that the pile-up of inventories and consequent de-stocking of the first two quarters was now over. Shipments by the sector during the first six months of this year showed GSM cards running at 200 million units, compared with 370 million units for the whole of the year 2000.

Opinions varied about the impact of the September 11 terrorist attacks on the USA. There was a widespread feeling that the industry would benefit from the increased interest shown in ID cards, both at the national level and for corporate security. Some senior delegates believe that the decrease in travel and consequent slackening in credit card spending will slow down the roll out of EMV cards.

Sizeable optical card order is won for border crossing

Btt November 2001

Drexler Technology has received a US\$4.8 million order for its LaserCard Triple-Image identification cards as

part of an ongoing US border-crossing ID card program. The cards – part of a five-year US\$81 million government procurement program for the US Immigration and Naturalization service – will be used by frequent visitors from Mexico to Texas, Arizona and California.

Under the terms of the five-year US government sub-contract, up to 24 million optical memory cards will be provided; the latest order is for deliveries averages about 200,000 optical memory ID cards per month starting in September 2001 and ending in March 2002.

Controversial face project goes ahead

Btt January 2002

Virginia Beach is the second city in the USA to approve the use of face-recognition surveillance technology. The Virginia Beach City Council voted 9-1 in favor of the technology. Council members said the city will establish an oversight committee to make sure there is no abuse of the cameras. The number of photos in the database will be limited to 2,500 known felons in the area, missing children or elderly residents and criminals suspected of frequenting the city.

Interest in biometrics rises following US Attacks

Btt Nov/Dec 2001

In the months following the terrorist attacks in the USA, biometrics seem to have rarely been out of the headlines, with many people in the mainstream media speculating about the numerous potential uses for the technology, including aviation security, border control and national ID projects.

Opinion polls have revealed a surge in enthusiasm from the general public

for biometrically-enhanced security – according to a Harris Poll conducted between 19-24 September, 86% of people interviewed said that they were in favor of the use of facial recognition technology to scan for suspected and known terrorists. In addition, the promise of valuable government orders for identification projects have helped to increase the value of certain shares.

Among the market highlights, three of the leading facial recognition technology companies, Visionics, Viisage and Imagis, saw shares leap. Visionics' stock, for example, soared by 90 percent when the Nasdaq reopened on Monday 17th September.

Months later and share prices for many of these biometric companies remain buoyant. Some commentators are urging caution, fearing the creation of a post-dot.com boom. They are pointing to the fact that many companies are barely profitable, and some analysts fear that "frenzied investors" may be expecting more from their investment than any biometric company could realistically expect to deliver.

Major bank signs up for dsv technology

Btt January 2002

A large number of banking customers in Israel will soon have their identities checked by dynamic signature verification (dsv) technology in a bid to increase transaction security and improve convenience. Following a four month pilot scheme, the country's largest bank, Bank Hapoalim, has given the go ahead to roll out the dsv technology at branches across the country.

Homegrown biometric company WonderNet will supply the technology, in a deal believed to be worth US\$2.5 million. So far, the bank has taken delivery at branches in and around the capital Tel Aviv. As Oren Grozovik, WonderNet's chief technology officer com-

mented: "There are approximately 330 main branches and we have installed around 1,000 of an estimated 5,000 seats."

Signature tablets are to be positioned both at the tellers' counters and on the desks used for more personal and business banking services. The system uses tablets from Wacom and uses WonderNet's PenFlow software. Used together the system is able to measure the three-dimensional motion of a proprietary pen above the tablet's surface and there is no need for the pen to even touch the tablet. (So it can be used to sign a piece of paper or a form positioned on top of the tablet.)

Biometric smart identity card for UK asylum seekers

Ctt January 2002

The UK's home secretary David Blunkett has announced that immigrants seeking asylum in the UK are soon to be issued with Chip Cards that will carry templates of their fingerprints. The Application Registration Card (ARC), as the Home Office Smart Card for asylum seekers is known, is intended to provide fast and positive identification of applicants subsequent to their initial processing at ports of entry or at the Croydon Asylum Seekers Unit.

The introduction of Chip Cards will begin by the end of January 2002. It is in fact the second phase of the UK government's overall Immigration and Asylum Fingerprint Program. The first phase followed the passing of legislation in 1991/2 that allowed asylum seekers'

fingerprints to be taken, stored and used for checking against fingerprint impressions taken on subsequent occasions.

The front of the ARC card will carry a photograph, a "ghost photograph", name and date of birth and date of expiry – plus a host of anti-counterfeit devices. On the back will be a memory chip, carrying two fingerprint templates. The Chip Card will be more expensive than a 2D bar-code card (which was also considered); but it will be future-proof in that its data can be updated.

Cash chequing operation closes

Btt November 2001

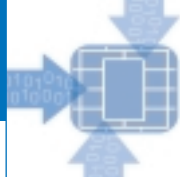
The economic downturn in the US has claimed yet another victim, as cheque cashing company InnoVentry announced its closure. The company, who's technology used facial recognition to identify individuals cashing cheques, had enrolled 2.5 million people, cashed 8 million cheques and installed 1400 machines. The company failed due to a lack of sufficient funding.

One source close to the company commented: "Before you get to the point of making money, you have to put millions of units out there. The problem with the InnoVentry model was that the installation of each machine cost US\$80,000 – and each machine only made a small amount per transaction.

Therefore it required numerous transactions to be successful. In a world where the US was doing well, it would have survived. As it stood, the company was spending US\$ 7-8 million per month."

The above news stories are brief excerpts from articles published in Card Technology Today (Ctt) and Biometric Technology Today (Btt).

Visit www.compseconline.com or www.biometrics-today.com for more information.



The Evolution of the Trusted PC

By the Trusted Computing Platform Alliance (TCPA)

In today's society we take for granted the technology of Computers; demanding flexible, advanced software programs plus secure ways of interacting with other Users. But this mix of requirements can sometimes be conflicting, and is not necessarily easy for the PC Manufacturers to achieve. This is why the TCPA (Trusted Computing Platform Alliance) was formed by Compaq, HP, IBM, Intel, and Microsoft; to standardize security and privacy levels across the whole industry, without compromising the sophistication and diversity of software.

Computing devices are now no longer restricted to PCs, with the advancement of PDAs, mobile phones and other handheld devices. With the increased interaction between such devices, Users are moving away from their own independent "safe" work stations, and are being networked together, either via the Internet or company networks. While this leads to an increase in transactions and available information, the downside can be a higher incidence of security breaches. It's been estimated that such attacks have affected business losses and computer management expenses by as much as 5.57% of gross revenues in 2000 (Omni Report 2001).

Currently, all that is available to combat security problems are add-on layers such as SSL (Secure Sockets Layer), PKI (Public Key Infrastructure), SET (Secure Electronic Transaction). However these applications are external to the main hardware platform and so do not provide security at the most fundamental level. What is needed is enhanced security at the level of the platform hardware, BIOS system software and operating system.

What is needed is a Trusted Client.

Trusted Client – The New Approach

In the past, manufacturers focused on PC security as an external issue, adding secure applications and software to their systems. Through Trusted Computing, the TCPA promotes a more integral solution, by first ensuring the integrity of the platform and then passing that trust through the different elements of the system.

Trusted Computing requires transactions and computing devices to be:

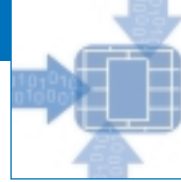
- Trusted — acting in a recognized manner and able to communicate what that manner is supposed to be
- Reliable — readily available for transactions and communications, as well as prepared to act against viruses and other intrusions
- Safe — able to stop unwanted intervention or observation
- Protected — sharing information with only those that need to know within commonly accepted parameters for computer privacy

The Trusted Client is designed to prevent the platform from logical, or software-based, attack. While the Client (or

Subsystem) can still be subverted by physical means, this mode of attack exposes only the secrets of the Subsystem on the local platform, and not on other connected platforms. In other words, if a Computer using a Trusted Client were to receive a virus, it could first of all notify the User that its software has been affected (not to be confused with anti-virus software that identifies and eliminates the virus, which is used as an additional application). Then the Computer could notify all other Computers on the network about the problem, so that no other Computer would access the infected system and spread the virus.

However, Trusted Computing is not only limited to protecting systems from attack, it also:

- Provides protected storage of cryptographic and sensitive data within the TCPA silicon technology
- Authenticates a computing device, verifying its identity to other computing devices
- Supplies owner-defined metrics for reliable, secure network environment access of only other trusted computing devices



How does this work in reality?

The TCPA specification advocates that a separate Subsystem (see Figure 1), can be trusted. The TCPA Subsystem is designed to provide reliable mechanisms for the measurement and reporting of integrity metrics, ensuring that the Client is Trusted. This consists of two building blocks:

- A Trusted Platform Module (TPM) defined as a secure controller (the hardware instantiation of the TCPA specification).
- Software to perform integrity metrics, in conjunction with the TPM.

To ensure system integrity for the Trusted Client, “integrity metrics” are used. These are defined as measurements of key platform characteristics that can be used to establish platform identity, such as BIOS, boot-loader, hardware configuration, OS loader, and the OS security policy. Cryptographic hashing is employed to extend trust from the BIOS to other areas of the platform, in the following simplified sequence:

1. The PC is turned-on.
2. The TCPA-compliant “BIOS Boot Block” and TPM have a “conversation.” This attests that the BIOS can be trusted.
3. BIOS queries to ensure that user is authorized to use the platform.
4. The BIOS then has a “conversation” with the operating system (OS) loader and the TPM. This attests that the OS loader can be trusted.
5. The OS loader then has a “conversation” with the OS kernel. When the OS kernel loads, it knows what software has had access to the system ahead of it. This establishes that whatever happens within the system from that point forward is 100 percent controlled by the OS kernel.

The core elements of trust that are built into the system through the TPM and BIOS extend their trust to the boot loader. The boot loader extends its trust to the OS loader. The OS loader in turn extends its trust to the OS, which can then extend its trust to applications. This process ensures that the initial point of trust (TPM and

BIOS) spreads the trust throughout the whole system, thus resulting in a Trusted Client.

About the TCPA

In 1999, five leading Hi-Tech companies (Compaq, HP, IBM, Intel, and Microsoft) formed an alliance, in order to introduce the concept of a common Trusted Computing Platform within the industry. Now there are over 160 members of the alliance; ranging from OEMs (Original Equipment Manufacturers) and PC Manufacturers to Semiconductor Manufacturers. The alliance is open to any company that can assist in the development and production of the Platform.

The TCPA set out to cover both security and privacy issues in its mandate, with the following mission statement:

“To maintain the privacy of the platform owner while providing a ubiquitous interoperable mechanism to validate the identity and integrity of a computing platform.”

The alliance plans to achieve this goal by issuing White Papers detailing its ideas on Trusted Computing and releas-

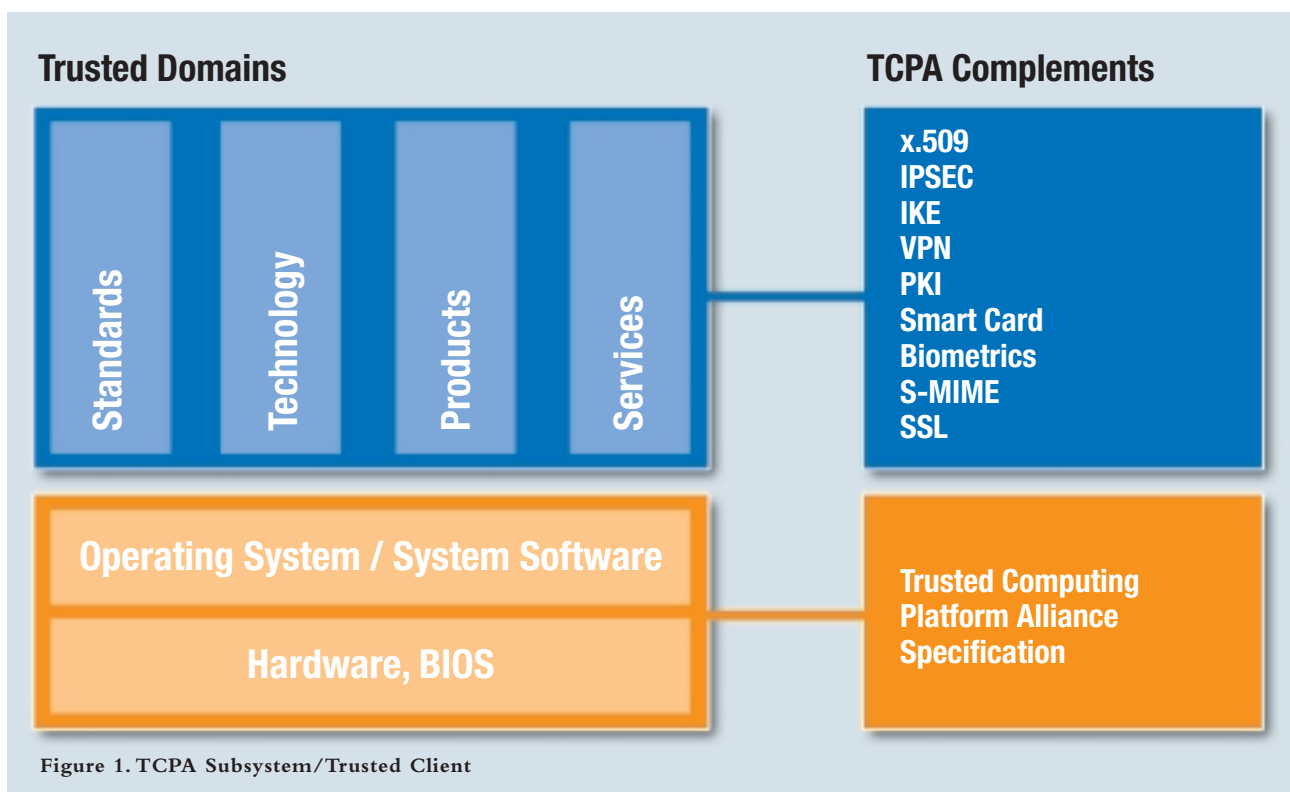
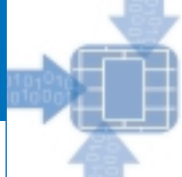


Figure 1. TCPA Subsystem/Trusted Client



ing the Specification for members of the alliance to follow when developing new products. The Specification has moved through different versions over the last year, with the release of Specification 1.1 in November 2001.

Summary

Although the alliance cannot at present guarantee a “hack-proof” system, it has

made significant steps to improve the previous security and privacy shortcomings within the industry.

By bringing together all the major manufacturers, time is no longer wasted on producing competing standards, rather, companies can use the TCPA Trusted Client Specification to enhance their own offerings.

Consumers then benefit from devices that they can trust; reducing the risk of security breaches and ensuring that they are dealing with the intended partner.

It is hoped that this new level of trust will further spur the growth of e-business and e-transactions and lead to a new era of trusted computing.

Examples of “Trust” in action

Remote Attestation in B2B/B2C

TCPA remote attestation allows an application (the “challenger”) to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure.

For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform is trustworthy. The service provider’s platform (the “challenger”) queries the remote platform. During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored.

When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy. If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger make the final decision regarding the trustworthiness of the remote platform.

(Taken from TCPA White Paper: Building a Foundation of Trust for the PC)

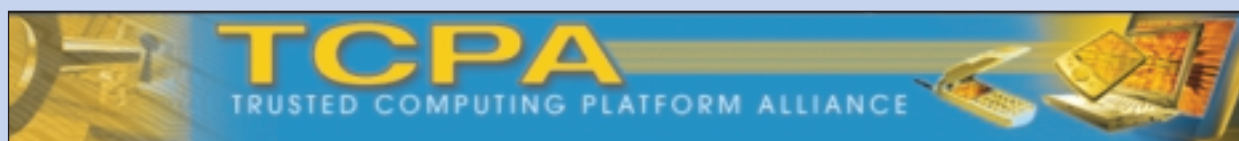
Ensuring Privacy through Authenticated Anonymity

Imagine that the PC has booted as described in the four-step sequence outlined earlier in the article, and that the system can be trusted. It is now possible to present credentials for the system to a third party. In doing so, however, the user exposes the identity of his or her platform to the third party, and possibly runs the risk of providing more information than intended.

An alternative is to use a recognized and trusted entity within the industry that can verify that an identity belongs to a trusted platform. This is termed “anonymous authentication.”

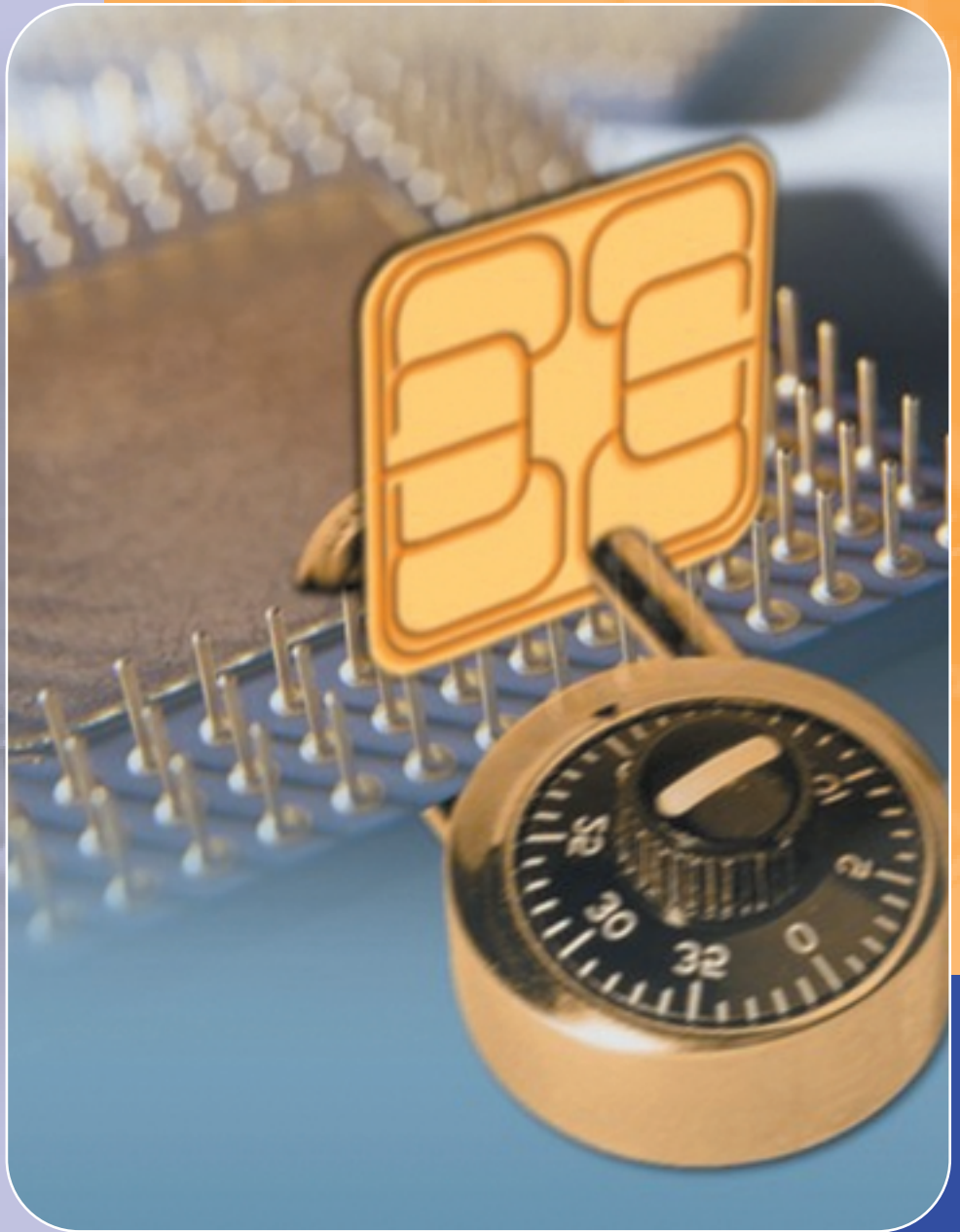
Here is how it works in a TCPA-compliant subsystem:

The user goes to a third-party Authenticated Anonymity Website (AAWS), and requests site verification. Using the TCPA Subsystem, the AAWS provides the user with credentials, known as a “cert” or certification. Those credentials assert that the platform is authenticated by a trusted third party and that the platform can be trusted in certain ways. The AAWS asserts that the platform is unique, but it will not tell someone else anything that can be traced back to the user. For the purposes of the transaction, the platform is reliable, and also anonymous.



For details about the TPM from Infineon Technologies, see page 60.

Security Embedded



www.scsquare.com

SC² Ltd.

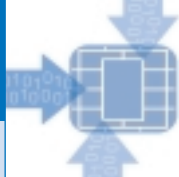
Security Chip & Communication

2A HABARZEL St. RAMAT HAHAYAL

TEL-AVIV 69710 – ISRAEL

Tel: +972 3 7657 331

Fax: +972 3 6494 975



Working Within TeleTrusT

By TeleTrusT

The non-profit organization, TeleTrusT was founded in 1989 and has been increasingly active internationally since 1997. The aim of TeleTrusT is to support the development and awareness of trusted information and communication technology. To achieve this, applications for trusted, forgery resistant and verifiable electronic business transactions are promoted.

The basis of TeleTrusT requires the co-operation of technical component manufacturers, algorithm and software developers, providers of secure services and end-users, ultimately resulting in trusted and secure information processing and transmission in public networks. TeleTrusT has over 100 member organizations and companies (some based outside of Germany), which are organized into 8 working groups and 4 projects.

The Working Groups (WG 1-8) cover the following topic areas:

WG 1 Legal requirements for trusted communication

WG1 was one of the first working groups to be founded. Early on it had become clear that electronic communication and data procession can have legal implications and that it is therefore necessary to further develop the legal system that has evolved over centuries for the paperbound world. TeleTrusT is known today at the Federal ministries as a competent partner for the accompaniment of legislative processes regarding information security, since as a non-profit organization TeleTrusT provides independent and objective comments.

WG 2 Security architecture and Smart Cards

WG2 is mainly technology oriented. Highly specialized experts from TeleTrusT member companies analyze threat scenarios and develop specifications. The Chip Card as a core element of a Personal Security Environment (PSE) is especially focused on. An example for this is the specification "OIC – German Office Identity Card", which can be obtained via the TeleTrusT

web site or main office. The most recent project of WG2 is "Evaluation BioCard" (see side bar for more details).

WG 3 Medical applications of trustworthy information technology

This working group represents an important application area. Medical telematics without trusted electronic communication is unthinkable, since the inviolability of the patient's secrets is a fundamental part of the mutual trust relationship between doctor and patient. The use of new technologies holds great possibilities; on the one hand cost reduction through the avoidance of unnecessary double expenses and on the other, gaining time and quick access to relevant information with a view to saving lives. Already in 1998 WG3 wrote the brochure "Crypto Report", which is available on the TeleTrusT web site as well as from the main office. The Crypto Report is the bestseller of the TeleTrusT brochures, since it explains in easy and understandable terms the basics of cryptographic procedures. Currently WG3 is working on a new edition of this brochure.

WG 4 Open e-commerce security

Working Group 4 is also very application-oriented. The activities of WG4 cover an area, which, with its many business processes in B2B and B2C, is of great use providing valuable information, based on experience for potential users. Recently WG4 published the brochure "Trusted E-commerce", which is available on the TeleTrusT web site and from the main office.

WG 5 Promotions

"Do good and talk about it" is a maxim of marketing. In the last years the main office accommodated the growing demand for public visibility of TeleTrusT. Marketing experts from the member organizations support the growing TeleTrusT activities in topic related teams.

WG 6 Biometrics

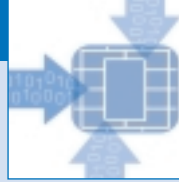
A few years ago biometrics started to develop as a technical innovation with clear opportunities in growing application areas. This was reason enough for TeleTrusT to pick up the development and carry it further. Today TeleTrusT is a competence association for applied cryptography and biometrics. This is underlined by the membership structure: currently about one quarter of members are directly or indirectly connected to biometrics.

Back in 1998 WG6 produced the brochure "Catalogue of Criteria", which serves on a working level, as a tool for potential users and operators of biometric procedures and applications. The brochure is available on the TeleTrusT web site or from the main office. Members of WG6 initiated the project BioTrusT (see side bar for more details).

WG 7 Public Key Infrastructures

Working Group 7 deals with all aspects of the deployment and operating of Public Key Infrastructures.

Main issues are the services offered by a PKI (integration of PKIs into business processes, their marketability), their organization and operation (deployment and process organization, key management, security concepts, policies) as well as the cooperation of dif-



ferent PKIs (interoperability, cross-certification, global aspects). Most recently WG7 has been supporting the project "Bridge-CA" (see side bar for more details).

WG 8 MailTrusT

MailTrusT is a system concept for end-to-end security for e-mail and file transfers based on internationally prevalent standards that were developed over the course of several years. Another main concern, as well as the security aspects, was also the interoperability of components from different manufacturers. Therefore, MailTrusT was the basis for the SPHINX project for secure and trusted communication between the government offices in Bonn and Berlin. To further support the spread of interoperable crypto-components in applications for different business processes, WG8 is now actively involved in the project "ISIS/MTT Test System" (see side bar for more details).

TeleTrusT also co-operates with other organizations, e.g. as an associate member of the PKI-Forum, ensuring that its work is influential internationally. Furthermore, TeleTrusT operates on a political level; the organization has advised German Ministries as well as the European Union. Therefore, in terms of the support of marketable products, influence has been exerted on the implementation of the European Guidelines in German legislation.

Since 1999, the annual European information security conference ISSE (Information Security Solutions Europe) is being organized jointly by EEMA – the European forum for e-business – and TeleTrusT. ISSE is supported by the European Commission and the German Ministry of Economics and Technology. Whereas EEMA handles the overall organization and promotion of ISSE, TeleTrusT chairs the international program committee and is thus responsible for the content of the conference. In 1999, there were 500 delegates in Berlin, 800 participants met in Barcelona to attend ISSE 2000 and this year 800 visitors attended the conference and exhibi-

tion in London. ISSE has now developed into the most important information security conference in Europe.

In order to support the presence of German information security companies in the international market, increased marketing and sales activities are necessary. Starting in 2001 TeleTrusT is organizing – with generous support from the AUMA (Association of the German Trade Fair Industry) and the BMWi (German Federal Ministry of Economics and Technology) – a joint booth of German companies at the RSA conference and exhibition in California, the biggest IT Security event worldwide. This will provide a platform to present German and European crypto products and at the same time stimulate the global know-how transfer.

TeleTrusT also supports scientific research and commissions external studies on the security and trustworthiness of public electronic information transfer. Scientific results are published, input is delivered to standardization initiatives such as EESSI, and workshops and presentations held to promote trusted information and communication technology. As a non-profit organization TeleTrusT is politically and economically independent and can therefore represent a purely objective viewpoint. The organization has also promoted the dialog between technical and legal disciplines, and between data protection officers, consumer protection associations, governmental and political institutions, furthering the discussion on the necessity of extensive use of cryptographic techniques to ensure information and communication security.

TeleTrusT promotes trusted information and communication technology in real-world applications. The interoperability of components and techniques, the warranty of their security and the consideration of their international compatibility are the basis for the development of specifications for components and interfaces. These theoretical considerations are tested in practice and made workable in projects such as BioTrusT.

Current TeleTrusT Projects

- ▶ BioTrusT is an international project testing the practical implementation of biometrics, accompanied by scientific research by the Technical University of Giessen-Friedberg. The project is supported by the Sparkassen-Finanzgruppe (Savings Banks Group) and the German Federal Ministry of Economics and Technology. Different biometric applications, based on various technologies, are tested in diverse application fields with regards to their reliability and robustness, as well as to the user acceptance. The results will be published after the conclusion of the project – estimated in a year's time. Further information on the project is available on the TeleTrusT web site and at www.biotrust.de.
- ▶ Bridge-CA is a project (open to international participation) that connects already existing, and operating PKIs. The project is pragmatic in its approach and is based on internationally recognized standards (S/MIME, X509v3). This year TeleTrusT took over the operation of the Bridge-CA, which was initiated by Deutsche Bank and Deutsche Telekom in 2000 and inaugurated at CeBIT 2001 by the Federal Minister of the Interior, Otto Schily. Further information on the Bridge-CA can be found on the TeleTrusT web site and at www.bridge-ca.org.
- ▶ Evaluation BioCard is a project initiated by Working Group 2. The task of this project (which is led by WG2 in co-operation with WG7) is the development of a protection profile and, if necessary, of further evaluation documents for Smart Cards and OnCard-Matching. Co-operation with GISA (German Information Security Agency) and an accredited evaluation authority is planned.
- ▶ In the project ISIS-MTT Test System, TeleTrusT and T7 (Arbeitsgemeinschaft TrustCenter) are developing a common specification for PKI based applications. This common specification is based on the specifications ISIS v1.2 and MailTrusT v2. Furthermore, a test concept and test specifications for proving interoperability of products and solutions for electronic signatures, authentication and encryption are to be compiled and published. The results are the basis for a test system for proving interoperability in practice.
- ▶ The project group Cardterminals has been in existence for several years now, developing specifications such as MKT (Multifunctional Cardterminal) and UCTS (Concept for Universal Chipcard Terminal Systems). Here, the main focus is given to the card terminal as a part of the whole security system of Chip Card based applications.



Market Trends and Hardware security for banking and brokerage applications

By Monika Bremer, Infineon Technologies AG



After the unprecedented hype for e-business transactions, the online world is changing once again. The first online business models focussed on the winning of online users. Access fees for online providing services and secondly web advertising with a correspondent click rate promised financial success. But the use of these business models meant that only in very few cases was money actually made. Fees for the online access decreased drastically while web banners have not lived up to their promise of a high yield (click rate) and the numbers of web sites in the last years grew faster in proportion to corresponding budgets for online advertising.

New solutions for successful online business models have to be created. The future will be dependant upon high valued content that the user is willing to pay for, e.g. personalised services, from which the user gains individual added value or e-learning and e-support. Only those businesses who possess, or who produce, high value content themselves, in combination with value added services, convenience for the user and personalized services, will be successful in the future.

But what does the future of the banks and online business look like? The online world for banking started with home banking and online standard transactions. The banks, in particular the direct banks, are moving away from the mere online trader offerings towards more of a global online investment house. The future of the banks lays in the extension of their offered products - online, and in the personalization of their banking services.

In the past, the online offering of banks and brokers was based on transactions in the financial and stock business: cash transactions, standing orders, buying and selling of securities. Their next advance was to extend the offering of their core business. Nowadays, everything considered a payment transaction is counted among the online banking business. Transfers and standing orders are commonplace, account statements and account abstracts, transacting saving agreements online, e-mail support, credit

card applications, credit calculations and news complete their online service offering. Due to the complexity of the security business in comparison to payment transactions, the brokerage business presents a much larger field. The buying and selling of stocks, fixed interest bearing shares (stocks, securities) and standard warrants are self-evident. These services are value added due to real time trading, where the broker sets binding prices online for a certain amount of time (e.g. 10 sec) and it is up to the customer to decide whether they agree to the price offered or not.

Today stock exchange information systems deliver real time prices, without time delay, directly from the trading floor. The bank itself often incurs these additional costs. With so-called watch lists customers are able to deposit the securities that they don't have obligations to in their depots but still watch the price quotations. Alert functions make it possible to inform the customer if a stock has reached a specific price, e.g. via SMS (Short Message Service). Further stock information e.g. of the company itself or news about the stock market and the economy, are taken for granted today. The customer registers online either an individual profile or selects directly from the services offered to get all relevant information with only one click. The ongoing trend is to represent all their products and services online and the winning of customer's loyalty with stock close services or the merchandising of prod-

ucts and services, which support online trading. Not only are customer bulletins counted among these services, but also subsidised offers of books, magazines and PC's with already installed online access related to the subject, are provided to motivate the customer to change from the customary distribution channel such as letter, fax or call center to the possibility of online trading.

But what is the motivation of the banks and direct brokers, to transact as much as possible online? The decisive factor is the idea of **"straight through processing"**.

Whereas the distribution channel of the branch, the call center, letter or fax communication still has a manual interface, today, at least, the processing of stock transactions without any manual interfaces is possible. From the input of the transaction data, through the execution at the stock market up to the accounting of the order, everything happens automatically. Until a certain capacity of the engaged systems is reached, the more transactions the better; for the costs of processing per transaction does not increase in proportion with the transaction revenues, which the customer pays through transaction fees.

But still, not all customers are convinced of the advantages of online business. A lot of them don't want to abandon the personal contact they have to the banks' employees. That is usually because



they feel unfamiliar with the new technology and systems they are confronted with. And in particular, for financial issues this can be a big element in not using the new online services.

Security aspects

The online banking and brokerage businesses started connecting customers to the Internet with PC and corresponding special banking software from the likes of BTX (Bildschirmtext) and AOL (American Online). Internet trading followed shortly after. WAP-banking (Wireless Application Protocol) is now also possible and in Germany a broker has just released a PALM-trading application for those customers who use PDA's. Eventually, in a few years, the use of the Internet with the correlating applications will be part of daily life worldwide and its usage will be as self-evident as the telephone is today.

Security and trust will be key factors to make online applications successful.

Asking the banks about security issues, one answer dominates: with our cryptographic software our banking is secure enough. This is correct, in that the banking software presently in use enables a secure transfer of transaction data from A to B. But software alone is not able to protect users, devices and the storage of data.

User authentication in the banking sector presently takes place with a PIN (Personal Identification Number), a TAN (Transaction Number) or sometimes with an Identifier (an added password using password-software). This software administers the data in general using a database. Successful attacks on PIN and TAN data show that the data protection by software alone is not sufficient.

Two components have to be taken into account when speaking about user authentication. On one side the bank wants to know if the legitimated account holder or a legitimately authorized person is really doing the transaction. The

banks and brokers rely on the customer's self-responsibility to safe keep their confidential access data. On the other side, the customer should be sure about the identity of the bank's online web site that they use for trades and services. The customer wants to know that the site they are using is not a manipulated one.

First solutions in the market have already been established. Through the use of PKI (Private Key Infrastructure) banks and brokers can now exchange encrypted data. This can be transaction data as well as customer related data or information. The encryption takes place by using a public key, provided by the bank. This data is only legible, if the recipients using their own private key to decrypt it.

Certificates, as a secondary existing market solution, can also be issued by trusted third parties (Trust centers or neutral third organizations like TÜV). The organization proofs and verifies the legitimacy of the customer and assigns an electrical certificate as legitimacy confirmation. This can be used as a digital signature in the e-business environment.

Biometrical identification aims to identify users by their fingerprint, which is recognized by a FingerTip sensor. This sensor, which receives the picture of the fingerprint, can be implemented either in a terminal or in a card. Thus, biometrics replaces PIN and TAN functions or may even be combined with them.

The fundamental, unsecured set up of PC's and mobile devices makes them very attractive for attackers, since the CPU (Central Processing Unit) does not distinguish between "good and evil"- meaning between user software and attacking programs.

Meanwhile thousands of viruses, Trojan horse viruses and spy programs like "Key Logger", (which records the keyboard entries of the user), are known about and in use. An initiative consisting of

leading manufacturers has been founded to check the security status of a PC by the user and as well by the Internet trader/bank before a transaction may be done. The goal of the "TCPA" (Trusted Computer Platform Alliance) is to implement a security module named TPM (Trusted Platform Module) on the motherboard of the PC. The TPM is, among other things, able to spot changes of the operating system or single program parts (e.g. home banking programs) and is able to alert the owner of the PC before the PC is damaged or altered. The secure execution of the booting can also be controlled by TPM.



Mobile Banking

The requirements for mobile banking and brokerage security concepts are of a similar nature: the customer, the bank or broker and the terminal to be used have to be authenticated securely and a secure data transfer has to be guaranteed. At the same time the platform and the mobile device have to be protected against software attacks.

Today every GSM (Global System for Mobile Communication)-mobile phone



possesses a SIM (Subscriber Identity Module)-card, whose microcontroller is used for authentication, serves for the login of the subscriber into the mobile network and furthermore generates an individual key for voice encryption for every conversation, which it then passes to the mobile phone.

For applications in the m-commerce arena, the SIM as a security microcontroller can take over further jobs such as authentication and data encryption; but as the SIM-card is handed out by the network operator, it cannot always be assumed that all wished-for banking applications will be integrated into the card. Interesting alternatives to the single multi-functional SIM-card are mobile phones that have added slots for further cards: known as Dual-slot-mobiles. They may have a dual SIM-slot for a dual SIM-solution or, as in the case of the Siemens mobile phone SL-45, a dual card slot, where a MultiMediaCard™ can be inserted. These solutions all require a security microcontroller, which can be protected against attacks and manipulations.

Due to more complex cryptographic solutions e.g. PKI, future security microcontrollers cannot abandon specific cryptographic hardware. The Infineon security microcontroller is tuned specifically to the needs of modern PKI-requirements, e.g. 1.024 bit RSA, 32 EEPROM. This coprocessor has been optimized for fast arithmetic operations with extreme high numerical value and is implemented into an integral security concept of the whole controller.

Form Factor

The Infineon controllers can be implemented into many different form factors. Due to the specific feature of the form factor, it is normally only suited for a particular use. To enable an optimal use of the aforementioned services, it is advantageous that the form factor for mobile banking and brokerage is both removable and has memory storage capabilities.

Basically, the hardware security has to be distinguished into the removable and the non-removable elements. The aforementioned TPM is implemented as a fixed feature on the terminal's motherboard and so is named as a non-removable element.

The following removable elements have to be distinguished:

- The SIM-cards are the main product of network operators. As owner of these cards they also define their functions and applications as it is in their own business interest.
- The Smart Card in EC-card-format according to ISO-norm 7816 is the current form factor in the market nowadays. Up to now the magnetic stripe dominated as form factor for data protection, but in the future it will be replaced by a chip due to new regulations for data security. The banks are still the owner of the EC-Cards when handing them out and so they define the functions, the running time and the recipient of the card. It would be preferable if these advantages could also be guaranteed for mobile solutions for banks and brokers.
- The Small Card as a form factor, for example, the Ingentix Secure MultiMediaCard™, fulfils the requirements for mobile banking and brokerage. Today's dual slot solution – the Secure MultiMediaCard – with its size of 32mm x 24mm x 1.4mm – is ideal for mobile device slots. It can be inserted completely into a mobile phone as well as into a PDA such as a PALM pilot. Since it is a removable element, it can also be replaced and recorded over, either on a PDA or on a laptop or a PC with a corresponding adapter.

In short, the Secure MultiMediaCard may be an alternative implementation of the WAP WIM.

The similarities to a Smart Card implementation are not by chance, since it is based on Smart Card technology.

Function and application of the Secure MultiMediaCard for mobile banking and brokerage

Ingentix, a joint venture between Infineon Technologies AG and Saifun Semiconductor Ltd., is a semiconductor company that produces flash memory-based mass-storage products, which are based on Saifun's NROM™ technology. The initial products include high-density standalone flash chips, MultiMediaCards and Secure MultiMediaCards. Mass storage based on solid-state NVM (Non-Volatile Memory) is much more reliable than mechanical storage elements – such as hard disks – and is key for all portable applications.

The MultiMediaCard is not only the smallest storage card world wide, but also extremely robust and light-weight, low-current, fast, well-priced and because of its standardized interface, a easy storage media to implement. It is particularly suited for the insertion into mobile devices like telephones, PDA's and e-books.

The MultiMediaCard, a mass storage product, is being developed with the functions of the Infineon security controller incorporated onboard, resulting in a leap from a simple storage card towards a multifunctional smart storage card. Furthermore the implementation of the controller SLE66CX322P on the MultiMediaCard, creates a Secure MultiMediaCard, meaning that the Secure MultiMediaCard with the controller functions will be adequate for today's PKI and digital signature requirements. Consequently, a whole range of possibilities are open for new services in the mobile banking and brokerage market.

PKI encrypted transaction data supports and accelerates today's software security. It is also possible for the acknowledgement of transaction data transfer, for example as a message, when the recipient has performed the decryption of the transaction data. All transaction data, the transaction (order, order time, order reference number



etc.) itself, as well as the execution report, can be securely stored on the card and, for example, be compared with the bank's online order book. In this way, the bank or broker raises the trust it has with its customers. The customer then is able to compare his activities with those of the bank in a direct and prompt way.

All data, which the bank provides for the customer in the future, can be offered as a download and so be read by the customer offline. It is even possible to change the terminal. If for example, the download at home takes place over fast ISDN/DSL-internet access, it can be stored on the Secure MultiMediaCard and then read offline on such devices as the PALM pilot. The offering

can range from stock exchange news to personalized services (Market information, watch-lists, portfolio-analysis, reporting tools, etc.).

Marketing Opportunities for Banking

A large storage capacity in a small media in combination with security functions can bring about many opportunities. For example, it is possible to furnish the MultiMediaCard with a label and to define the date the card expires. In this way the bank or broker can issue the Secure MultiMediaCard, yet still remain the owner of the card and therefore in a position of defining the card's applications. The bank also has the possibility to install its own soft-

ware as well as both on and offline updates on the card. In this case, the customer is, with this banking software, also mobile in terms of key applications for trading, stock exchange information systems, news and services that require application-specific software.

If the bank or broker offers its own services for download, for which the customer might have to pay a fee, then a copy protection of the data is in the bank's interest as digital rights management for all data stored on the Secure MultiMediaCard is evident.

Conclusion

The changes of the online business models require new security solutions. The protection of high value content is getting more and more important, since the banks and brokers offer their services online and transactions are done via a mobile device – and so are interesting targets for attackers. Different form factors, into which the Infineon microcontroller can be implemented, are possible solutions for the increasing demand for security of data, user and device.

Due to its special features and characteristics, the Secure MultiMediaCard is able to protect not only the data and the device in use, but also guarantees the identification of the user/trader himself. Due to these capacities, one could say that the Secure MultiMediaCard is a real security solution, that fulfils not only all requirements of the mobile banking and brokerage business, but also facilitate value added services, both now and in the future.

SIEMENS

He uses his girlfriend's name as a password.

His PIN is written under his keyboard.

She doesn't need any passwords or PINs.

Siemens ID Mouse® – because there's only one effective security device for PC access: your fingerprint.

As soon as you touch the high-quality fingertip sensor integrated into a standard PC mouse, your PC lets you – and only you – gain access. The Siemens ID Mouse is easy to install, easy to use – right or left-handed – and is extremely reliable. So forget your passwords and PINs and let the mouse make things much easier. Further information on the Internet at www.siemens.com/biometrics (Europe)
www.siemens.co.jp/idmouse (Japan)
www.siemensidmouse.com (USA)



mobile business

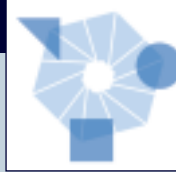
It's all about Identification...

By Marcel Hametner, Infineon Technologies AG



“Identification” as market segment is reported to have the largest smart card segment potential, which is something that Infineon Technologies takes very seriously as it means an enormous revenue return over the long term. Being responsible for our approach towards this market segment, I was asked to write about “Identification”. The article was to include a quick overview of what the segment is all about and describe briefly how this segment will change over the next few years.

However, if I were to go into depth on any one of these markets, I could spend the entire article on it (similar to an article on banking, GSM or transport). This approach, unfortunately, would not bring the reader much in terms of the whole segment itself. Instead, I will try to do justice to the article by outlining the complete segment itself, the market, and some of the technologies out there. Primarily, I will focus upon business models being satisfied by silicon-based solutions for the ID Market.



What is the ID segment?

“Identification” can be defined as a “token” containing information about the entity to which it is assigned. Let us briefly analyze what is meant by the 3 main topics in the definition: **token, information and assignment.**

The **token** can be found in various forms. As bar codes, pictures and/or diagrams (as a graphic identifier), in paper or plastic cards, stickers or labels, key rings (as a physical identifier) or even in smart (chip) forms of the aforementioned examples, as a more intelligent version. The **information** contained in the token can also be classified in various categories. For example; in the assisting of the verification of the identity of the entity it is assigned to, the listing of what the entity is permitted to do and how long that permission is valid for and finally, the storage of information describing the entity; its attributes, its function and so on. The **assignment** means that the token is personalized with a unique characteristic of the entity that is to carry the token. (For example the name or fingerprint of the person; the breeding details of a cow or the ownership and destination of a box of documents).

Simply put, the ID market segment can be summarized into functional categories as can be seen below.

- ▶ Citizen national ID
- ▶ Citizen national multi-application ID
- ▶ Passport
- ▶ Corporate & student access control IDs
- ▶ Corporate & student multi-application IDs
- ▶ Licenses (e.g. driving & firearm etc)
- ▶ Permits (e.g. pet, work, visitor, parking etc)
- ▶ Health & Insurance ID
- ▶ Social Security, Welfare & Pension ID
- ▶ Loyalty & membership cards
- ▶ Animal ID & verification
- ▶ Track & trace of articles/goods
- ▶ Device & terminal security/integrity
- ▶ Biometric Access
- ▶ Other

However, when talking about the size of the market, one must differentiate between **total market, total available market (TAM) and served market.**

Most statistics concentrate only on available market. Unfortunately, this does not provide an indication of the potential business, but rather encourages market share battles between competitors in a “perceived” market space.

To illustrate the difference in market size, I will take the example of Citizen ID (whether it be a card or not). The **total market** (defined as citizen ID world market) would be in the region of approximately 6 Billion units. However, this market is reliant upon all citizens on this planet carrying an ID Card. As we know, this is not the case (particularly one with a Smart Chip onboard). Therefore, if we were to look at the **total available market** (defined in this case as all service provider projects i.e. all Smart Card citizen ID projects) we would see that the number falls significantly to approximately 250 Million units. Furthermore, if we then focus in upon the **served market** area (defined as projects of service providers that are to be supported – a strategic focus upon a particular product line) the number falls again to round about 130 Million units. These numbers are only being used to illustrate my point, however you can see that there is an order of magnitude difference between the total market and the available market. One can clearly see that much work can be

done to increase the volume of the available market, increasing the market arena for silicon based smart solutions. One could imagine that this could be achieved through various means, including aligned lobbying activities by technology providers, solution providers and systems integrators, exploitation of successful case studies as well as sharing of IT infrastructure. If this example does not provide enough incentive, one can stretch the imagination and claim that each person normally has 3 types of identity cards thereby increasing the potential long-term market to a mere 18 Billion! The total market for **asset tagging, track and trace** of articles, **animal ID** and verification as well as **device and terminal integrity** is similarly astronomical.

Prevalence of large scale projects in the market place

People often ask why large-scale ID projects or large scale banking projects are not already prevalent in the market place. While I will attempt to explain the current circumstance, the good news is that the interest in silicon-based technologies in these markets has increased tremendously over the past 18 months (from a handful of projects to well over 100 world-wide). This trend is deemed to continue aggressively as projects in progress are due for completion in the near future.

The reason is not, as many people presume, the result of technology. It would





appear to be more about the perception of what the technology can do and how it should be implemented. One should take note that a Smart Card is not a solution, but rather **an enabler for a solution**. The result has been that if the problem or requirement is not defined correctly the solution will not work optimally and, as a consequence, the business case will fail.

For the most part, implementing new innovative solutions is all about easing the cost burden and creating revenue – plain and simple. Plain it may be. Simple, unfortunately, it is not.

Decision-makers today have minimal knowledge concerning the technologies they are investing in, with an

Profitability of the Scheme

It is true to say that since most schemes “need” to be built from scratch, the initial capital investment to set up the infrastructure is significant. The significance is normally beyond the medium term return on investment of a single application. At the moment, people are struggling to justify the cost on a business case designed for one or even two applications. Even cards of national interest can burden the pocket of the taxpayer. There is, of course, the tremendous shared cost benefit of the multi-application card. However, while the concept of multi-application is very attractive, non-technical conflicts between partners tend to halt the entire process.

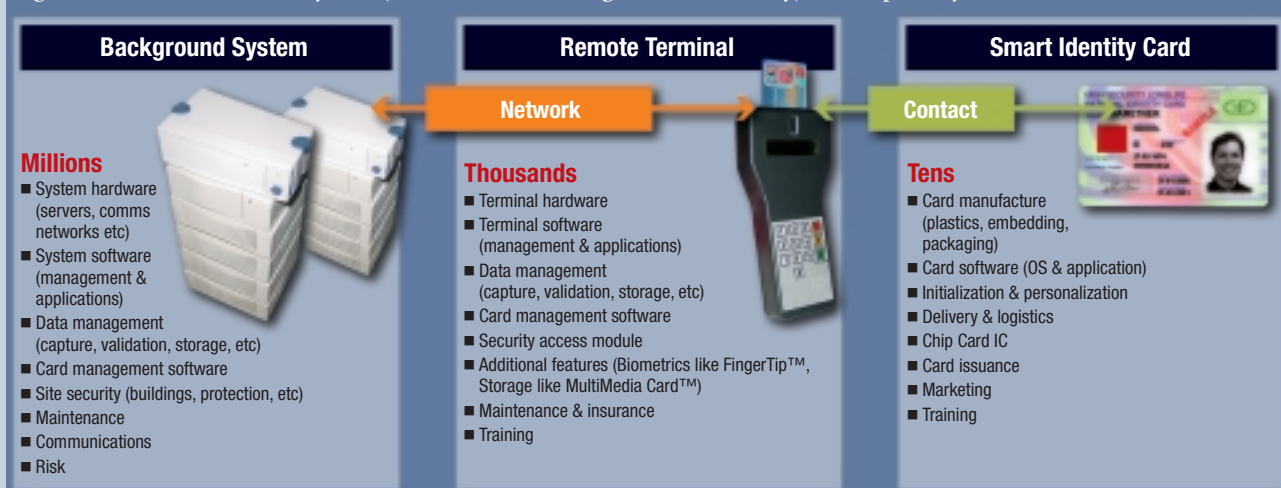
- 1) They actually were trying to provide a service to the consumer
- 2) Linking up their networks enables that service to transcend any single operator’s boundary.

Ok, I admit the contract subscription and transaction fees eased the business case, but the point is that it is possible to share the infrastructure cost and still have one’s own consumer interface. This in turn creates a business case for all. Nevertheless, branding conflicts are probably going to remain with us for some time.

Security

Awareness of security and its various uses and benefits is still a large hurdle

Figure 1. Cost Elements in a system (hardware, software logistics and security) – example only



appropriate education process sadly lacking, in most instances. For this reason, the problem or requirement is inappropriately fulfilled. I am of the opinion that it is the responsibility of the solution provider to pass on as much knowledge to the customer as possible. This knowledge should include not only technical information, but also a breakdown of the possible benefits and value that these technologies provide. An informed choice will assist the market to grow as a result of more successful projects.

Three additional hurdles that need to be overcome are **profitability of the scheme, branding, and importance of security**.

The technologies are becoming more cost effective and allow for a more flexible business case (a typical price / volume relationship). Typical cost factors are illustrated in Figure 1.

Branding

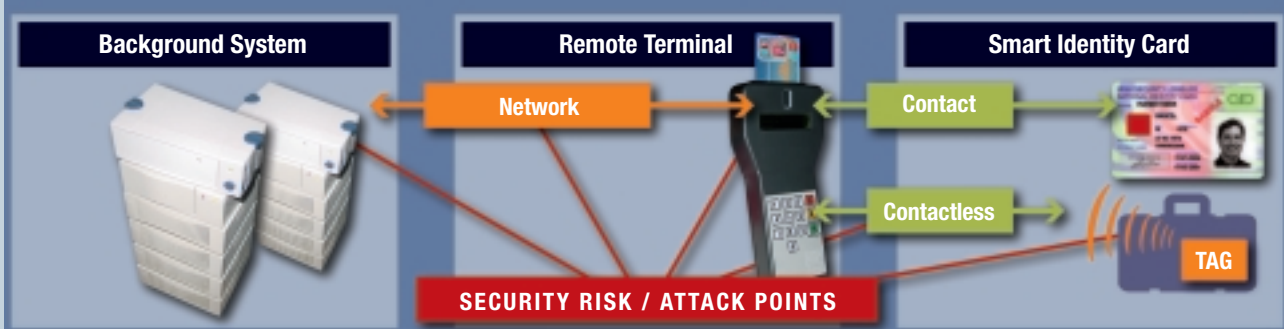
One of the conflicts on multi-application cards is the branding of, or the advertising on, the card that at times can cause the total shutdown of the project, with neither side winning. Taking the example of a GSM SIM card or a banking ATM infrastructure, one can illustrate that the operator can “own” the end customers and still retain their own branding and identity. These schemes worked for two reasons:

that requires addressing. On the brighter side, the market interest in the topic is slowly gaining momentum. Security is an intangible asset. For this reason it is difficult to quantify in monetary terms and so people are not necessarily willing to pay for additional security. The closest one gets is to use risk analysis techniques and insurance calculations that indicate cost through loss, theft and damage. Using these indications one can convince someone to pay for something that he can never prove to have prevented the threat it was designed for.

Unfortunately, security is only tangible when you lose something through the lack of it.



Figure 2. Security risks and attack points of the hardware



Silicon based “smart” solutions provide a level of security an order of magnitude higher than existing secure paper and print technologies. The combination of the two resolves many of the fraud and counterfeit issues on the cardholder interface.

There are various ways to resolve security concerns and ensure the integrity of a system. Some solutions from Infineon Technologies and their customers and partners can be seen in Figure 3.

Medium Size Projects and other Technologies

Device integrity

Device integrity includes topics such as having a secure or trusted PC, point-of-sale, ATM or mobile terminal about which one can feel confident enough to carry out electronic commerce or transactions. Here the project prevalence is reasonably straightforward to explain:

- 1) There was no urgent requirement
- 2) There was no cost effective mass-market type of solution.

This will change as the world moves into an even more mobile environment. Even developing nations can leapfrog technologies into the world of contactless information exchange and virtual networks. The most prevalent business models are that of fraud and hacking prevention. Unauthorized copying of electronic data is not easily identified or prevented since you still have the data, making the business case quite tricky.

Asset Tagging (Track and Trace)

Being able to track and trace assets such as original important legal documents, patents, government bills, engineering designs and the like, is a need that was not urgent enough before. The advent of time pressure, transparency and proof of originality has caused a search for convenient and cost effective solutions. While many types of solutions for each

one of the aforementioned topics have been in the market place for quite some time, their focus was on extremely niche markets. New IC technologies now make it possible to “label” lower cost items. However, the business model is based on time saving and not necessarily money creation. This is not determined easily. Even so, who would have thought one would track beer barrels using smart solutions?

I trust that the “bleak” outline in the previous paragraphs have at least indicated that the various markets are only in their infancy. Each application segment will grow tremendously should some thought be given into making the initial project a success.

The National Electronic ID Card – an Example of a Business Model

Since I represent a technology provider and not a systems integrator, I will not

Figure 3. Using secure Infineon hardware platforms and software

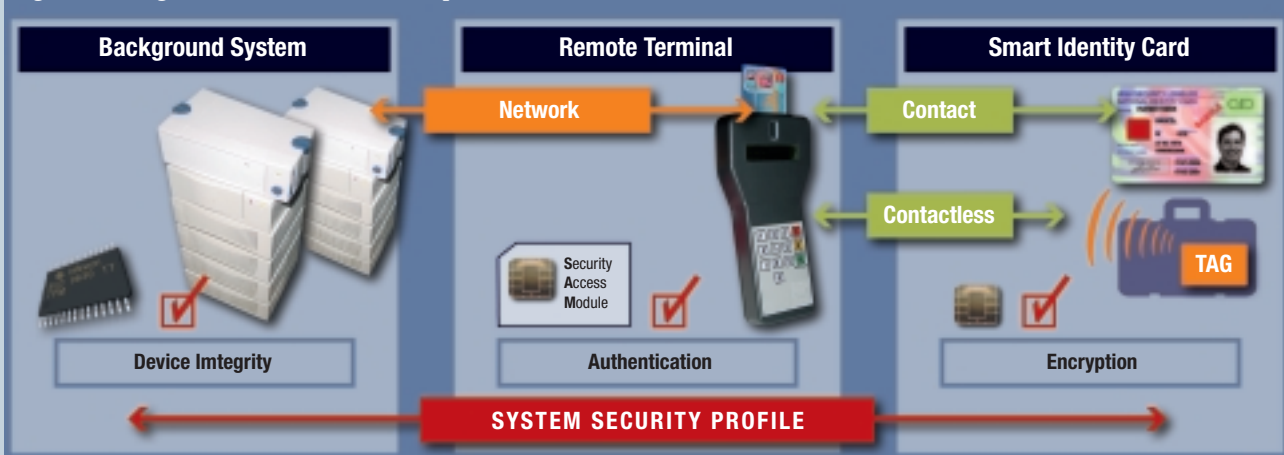
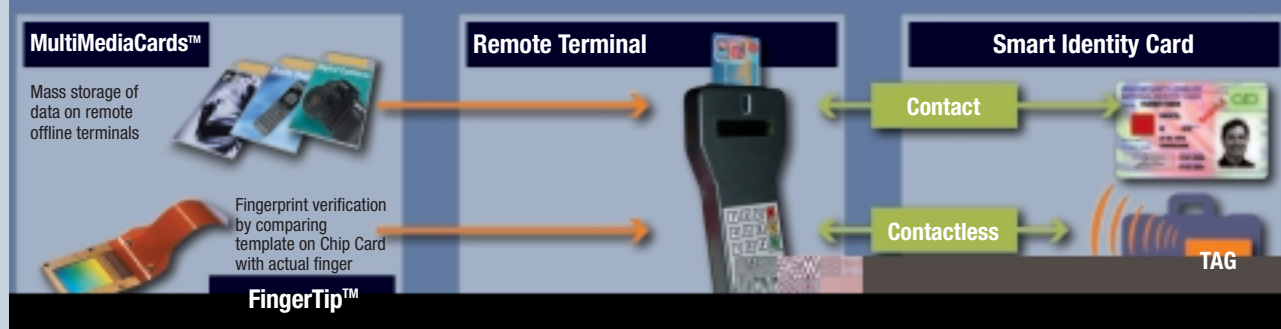




Figure 4. Adding functionality to the system to enable service delivery



dwelling on system issues. Suffice to say that the system definition and requirement analysis are critical to the success of any scheme. Smart solutions provide the benefit of convenience and mobility. I would like to highlight one example of a business model in the ID segment: **The National Electronic ID Card**. Through this example I will endeavor to illustrate various functionality and business case elements that become possible with smart solutions.

What is actually needed?

The Service Provider (i.e. government) needs a cost effective and convenient control and administration of the population, an increased level of data privacy and integrity and limitation of access of the population. The Public needs a convenient, safe and secure on- and off-line verification of their identity, a cost effective and convenient service delivery and an increased level of secure storage of private information

How do we satisfy these requirements?

Resolving these needs requires a convenient and secure token or mechanism to **verify** the identity of a person. Additionally one may add **permissions**, their **validity criteria** as well as **securely store data**. In order to verify that someone is who he or she claims to be, one needs to compare something that he or she has been given (by a trusted 3rd party) with something that he or she is.

For example: an identity card combined with a physical attribute, such as a fingerprint. In the case of verifying the location of goods, smart tagging tech-

nology possibly will lead to more secure logistics management using electronic article surveillance.

Technology used to resolve the service provider need(s)

How can a government minimise paperwork; reduce inaccurate data transfer and efficiently deliver services while at the same time cover an increased security network with existing resources? The answer would appear to be the introduction of a flexible and scalable smart system allowing the update of population statistics upon issuance, with the possibility of on- and off-line distribution of existing and future services. This system would also mean the ensuring of authenticity of the identification token as well as the convenient offline verification of a person (e.g. using remote terminals for execution and delivery of services).

Technology used to resolve the public need(s)

How many times have you waited in queues to register for something, filled out forms with your name, address, date-of-birth (in triplicate) or wasted time in duplicating your personal information only to have the service provider make mistakes in copying your personal details? If one could carry a convenient electronic version of that data, one can save time, money, and aggravation. Smart Card ICs, it would appear, are a viable solution to these problems and help to go some way to resolving the needs of the public.

This technology is the heart of any future identification token or mechanism of both people and goods. Within a chip

the size of a match head, Infineon's technology brings together the performance and functionality of a personal computer and the highest level of security evaluated to date. This enables their customers to create innovative solutions for the growing market.

Other innovative technologies such as biometrics and secure data storage devices add functionality, convenience and further levels of security in a smart solution.

In order to establish a particular system, various decisions and questions should be carefully considered and asked. *Figure 5* shows how in the case of a Smart Card solution, these would include hardware/software selections.

Implementation will only be successful through win-win relationships. These relationships will include the selection of reliable global partners to implement the solutions necessary to resolve the problem at hand, as well as reliable global partner networks to ensure minimal conflict in interaction and interoperability. There will also be the need to make use of economies-of-scale and scope where possible to increase buying power.

There will also be the need of a proven success history to prevent "reinventing the wheel" (e.g. security evaluations and customer references) as well as a history of innovation to ensure a reliable roadmap and future upgrades. But probably most importantly, an assurance of win-win relationships with sound business cases for all partners. One should also note that each type of project is influenced by many regional, environmental and competitive factors. The market is dynamic and thus flexi-



Figure 5.
Smart Card Solution – Hardware and Software Selection and Decisions Required for the System or Scheme

Hardware/Software selection	Decision to be made
System and infrastructure to control and administer the processes and data. The system will define the reach and scope of the project (one assumes a strategy has been drafted and the business case defined)	How widespread should the service extend?
Security profile to ensure system / scheme protection. Security profiles help define the implementation and risk of the applications and services.	How important is security to the scheme? What risk is the scheme able to carry?
System application including the system management and data storage software. This defines the functionality that will be provided by the system.	How will the scheme solve the problem?
Service delivery mechanisms e.g. deployment of terminals and training of operators.	How will the service be delivered to the consumer?
Communication method (contact or contactless).	What kind of maintenance and convenience is necessary?
Card Application functionality and memory space required (keeping future needs in mind)	What functions and services does the scheme want to deliver?
Card operating system to control the functionality of the card	Does the scheme need an open or proprietary solution for flexibility, scalability and security?
Chip Card IC. Select the hardware performance necessary (with regards to complexity, security and functionality).	Will the chip selected satisfy the need of the scheme?

bility is key to making the most of available opportunities.

Final comments

In the ID game, if people were to really think about what service and value they could provide the consumer with (irrespective of the infrastructure, since

it must be there anyway), the business case will work. Generally, consumers pay for convenience and perceived value. In order to make larger schemes feasible one could join forces on infrastructure spending and create a platform from which many applications can find a business case. If the analysts could agree on the application seg-

ments they will measure, a clearer picture of the market can be formed. Currently there are no benchmarks or reference statistics that make comparison convenient. This clearer, more detailed information will allow all competitors to improve their market insight and promote silicon-based technologies for the benefit of us all.

press-release by G&D

All on one card – Macao pioneers citizen's card

Giesecke & Devrient partners with Siemens to implement a smart ID card · 42/2001

Munich, January 8, 2002. Over the next four years, technology group Giesecke and Devrient (G&D) will be sub-contractor to Siemens in supplying smart ID cards to the citizens of Macao. A total of 540,000 inhabitants of the former Portuguese dependency, returned to the People's Republic of China in 1998, will be issued an ID card incorporating a chip. This smart ID card comprises biometric identification, a digital signature function and a payment application, and in addition can be used as a driver's license.

This is the first time anywhere in the world that a genuinely multifunctional card is to be issued as an identification document. G&D has contracted to supply the card body, the chip operating system and the basic applications such as the digital signature and biometric features as well as the personalisation equipment and the complete data logistics functions – a package equivalent to 80% of the total solution. The overall project will bring in a revenue of US\$ 14 million, with G&D's share worth around US\$ 11 million.

For more information please contact:

Giesecke & Devrient GmbH, Andrea Bockholt, Press Officer
Prinzregentenstrasse 159, D-81607 Munich, Tel: +49 89 41 19-2422, Fax: -2020
eMail: andrea.bockholt@gdm.de, Internet: : www.gieseckedevrient.com

Multi-Application Card Controllers Go 32-Bit

By Bernd Meier,
Infineon Technologies AG

**Infineon's 88 Family
for next generation Smart Card security.**

Today Smart Cards can be found in GSM SIM cards and banking cards, although the functionality is very specific and the number of applications per card is very limited. Any mainstream hardware out in the market tends to be based on 8-bit controllers with memory configurations of up to 32 kByte of E²PROM, 136 kByte of ROM and 6 kByte of RAM.

However, the evolution of the Smart Card is currently going in a new direction. The major trends in the market for Smart Cards are for those cards with enhanced services, with the capability of executing multi-applications on a single card. Additionally, the issuer of the card wants to offer the possibility of downloading new applications and functionality to the card - in the field. The software implementation available today is based mainly on a proprietary operating system with embedded applications. Together with the trend for multi-applications, the market is starting to demand open platform systems, based on virtual languages, like Java SCTM. The idea behind this is to separate the operating system and the application software in a standardized way, which will finally allow different parties to write applications for various numbers of services.



The SLE88CX720P

The SLE88CX720P is the first product in the 88 Family of Smart Card security controllers. This new security controller family incorporates a dedicated 32-bit Smart Card core with heavily increased security and performance, and reduced power consumption. Offering high performance at lowest power consumption, the controller family is well suited for both contactless and contact-based applications.

The SLE88CX720P provides a platform for modular operating systems supporting multi-applications. For instance, the controller has a complete new Memory Management and Protection Unit (MMU) that serves as a firewall to enable secure separation of adjacent application programs and data. Furthermore, the MMU is the hardware basis for secure downloading of applications in the field, even after the initial card personalization. A very quick and efficient context/application switching mechanism allows fast switching between multiple tasks. This flexible MMU concept also shortens development cycles for additional applications. A Smart Card dedicated 32-bit RISC core achieves the high execution performance of the CPU. Efficient support and an additional performance increase of multi-application schemes are gained by a hardware acceleration of Virtual Machine languages like Java SC, MULTOS™ or WPSC™.

The product covers the voltage classes A-C of the 3rd generation specification for mobile communication TS31.101 (which means 1.62V up to 5.5V). The IC offers 240 kByte of ROM, 8 kByte of user RAM and 80 kByte of E²PROM. The virtual address range of the MMU is 4 GB. Program and data modules are organized as packages. Each package has a defined memory range of 16 MB and dedicated access rights.

A number of powerful peripherals offer hardware support for time and code intensive operations. The Advanced Crypto Engine (ACE) is equipped with its own RAM of 700 bytes and supports all of the known public-key algorithms based on large integer modular arithmetic. It

allows fast and efficient calculation of, for example, asymmetric cryptographic algorithms like RSA operations with key lengths of up to 2048 bit. For symmetric crypto operations, a DES accelerator supporting Triple-DES is implemented. Using the ACE and DES module a secure transmission for downloading of additional applications can be ensured.

As security is the first priority for any new core designs, Infineon Technologies integrated an entirely new security concept (instead of adding additional security features to an existing design) for the SLE88CX720P - this security controller takes a quantum leap forward in terms of improved on-chip security. A variety of different trap vectors inform the operating system about exceptions (e.g. access violation).

The Key Benefits for Multi-Application Smart Cards

The increased growth for multi-application Smart Cards has meant that there has also been an increased demand for a more powerful CPU, as well as secure memory management. The 32-bit arithmetic logic unit and the high internal clock rate of the SLE88CX720P easily provide sufficient performance to cope with multi-applications. Special hardware features accelerate the execution speed of the active application; e.g. the data and instruction caches speed up the memory access and the hardware-implemented context save mechanism allows switching between different functions, tasks or applications in a very fast and efficient way.

The Virtual Memory System

The virtual memory system of the 88 Family provides an extremely convenient programming model for the software developer. The 32-bit design of the 88 Family architecture provides 4 GB of linear address space in virtual memory. Virtual addresses are translated to corresponding physical addresses by the 88

Family's memory management unit using a page table cache. All possible virtual memory addresses are mapped to addresses in physical memory for delivery to customers in a "tree" structure. Part of this tree is cached in a page table referred to in the SLE 88 Family as the translation **lookaside** buffer. It stores a limited number of virtual-to-physical address translations to accelerate accesses to physical memory.

Another, smaller cache known as the package descriptor buffer is also pro-

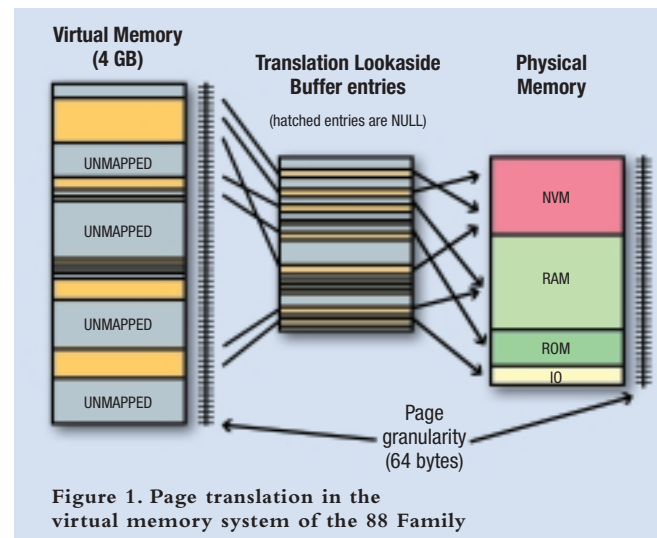


Figure 1. Page translation in the virtual memory system of the 88 Family

vided to hold information for locating the appropriate virtual-to-physical address mapping if no entry for the relevant address is found in the **translation lookaside buffer** (TLB). The entries in the **package descriptor buffer** (PDB) are called package descriptors, compliant with the package concept employed by controllers in the 88 Family. Using the information held in the PDB, the tree structure is traversed in a "page table walk" to locate the physical address corresponding to the specified virtual address. The TLB is then updated with the new entry. If the relevant package descriptor for a virtual address is not available in the PDB, the operating system has to provide the appropriate mapping.

The translation lookaside buffer stores page table entries specifying a virtual page and its corresponding physical address along with the access rights associated with the address. *Figure 1*

schematically illustrates the translation of virtual pages into physical page frames using the TLB. Besides the non-volatile memory (NVM), ROM and RAM regions, an IO region (for handling data related to peripherals and for storage of system registers known as special core function registers) is also mapped to virtual memory.

Why Use a Virtual Memory Concept?

The virtual memory concept deployed in the SLE 88 Family architecture offers the following advantages:

- ▶ The virtual memory mechanism may be used in the TLB to scramble the pattern of page frame addresses of applications. This makes it very difficult to tamper with certain logical locations in the data or code regions of an application, because the corresponding physical locations are controlled by the operating system, and may even differ from card to card.
- ▶ The 88 Family architecture supports uploading and deletion of card applications in the field. This would normally lead to fragmentation of the NVM area. The virtual memory concept means that no defragmentation is necessary: the application sees only the linear, virtual memory space and not the actual physical memory.

tation is necessary: the application sees only the linear, virtual memory space and not the actual physical memory.

- ▶ The full virtual address space is available to the code and data of an application. With the virtual memory management concept, packages do not have to be relocated during uploading or at runtime. Each package may be compiled off card to start at its specific address.
- ▶ Defective ROM, NVM or RAM pages may be substituted by working pages during a controller self-check after a reset. Then the TLB page table entries need only to be modified.

The Package Concept

Along with the demand for multi-application cards, the need for secure software implementation has become mandatory. If the card operators will offer field updates, there is the need to define who exactly is allowed to download additional software to the Smart Card – which means that the functionality of the whole card has to be guaranteed.

The 88 Family architecture offers a package concept. This concept allows

security-sensitive parts of code and data stored in a library to be isolated from other libraries in the same application in so-called packages. In this way, the workstation programming model for multiple interacting libraries in a task is used, but with full security. The 88 Family provides an extremely high level of architectural security.

Another benefit of the package concept is that the security certification process for functional additions to a certified library is made easier. The entire updated library does not have to be re-certified, but rather only the packages containing the new additions. The software development tools are designed in such a way that security features in the 88 Family are transparently supported for programmers.

This package concept effectively provides hardware-controlled cooperation between libraries in a single virtual address space. A package needs only to transfer control to another package by calling a function in the second package, which returns to the original package after the requested function is finished. Hardware is used to protect selected parts of a package's code and data against access by other packages. Figure 2 shows the package concept of the virtual memory system.

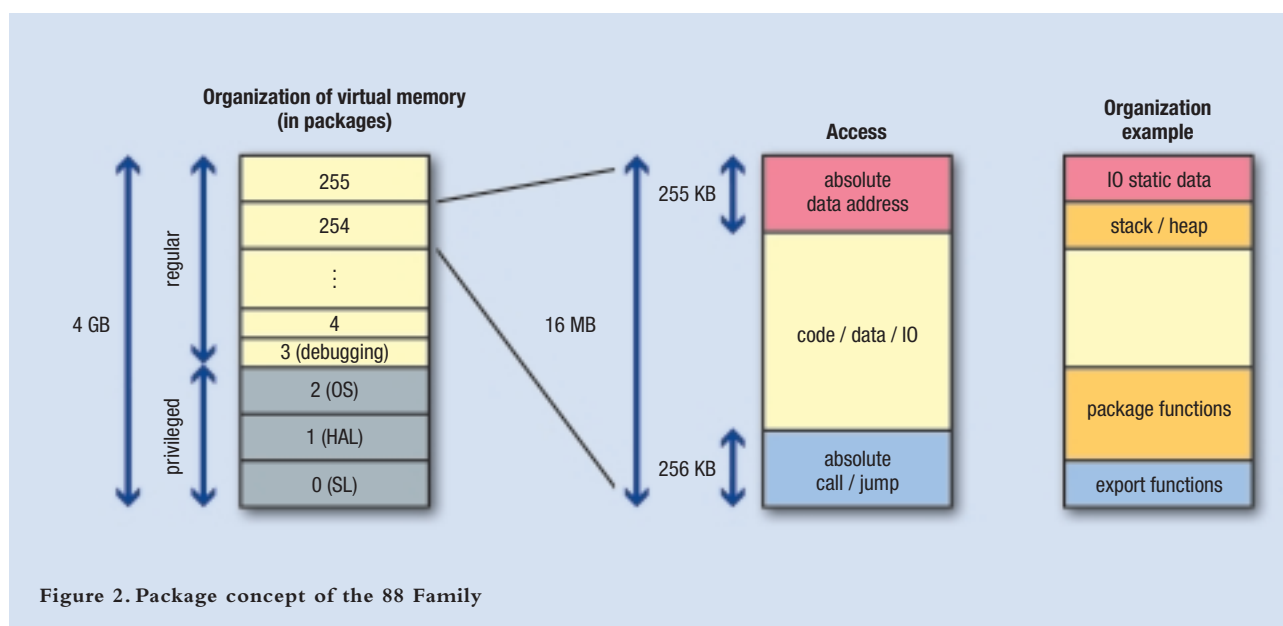


Figure 2. Package concept of the 88 Family



Summary

The SLE88CX720P fully supports the requirements needed for real multi-application operating systems. It allows secure operation of SIM/USIM, banking, access control, loyalty, Pay-TV,

health care and identification applications – all in one chip.

The advanced technology, the highly developed security concept, the low power optimized 32-bit core (support-

ed by various powerful peripherals), and the possibility to adapt the performance to application requirements, establish the foundation for meeting the requirements of a completely new (and exploding!), Smart Card era.

Unsurpassed Computing Power and Leading Edge Security Capability for Multi-Application cards

Infineon Technologies' security controllers in its 88 Family are designed for multi-application Chip Cards used in electronic banking, mobile communications and identity authentication, and combines high-performance 32-bit core architecture and an integral security concept to meet the demanding requirements of multi-application systems. The first IC in the 88 Family, the SLE88CX720P, sets a new standard in performance and flexibility for Chip Card controllers. It optimally meets customer requirements for large fixed and re-programmable memory, Virtual Machine Language acceleration to execute application code written in JavaSC and other stack-oriented languages. Simplified software development facilitates faster time-to-market, and exceptional security functionality adds further customer benefits. The IC is based on a 32-bit RISC CPU running at frequencies of up to 66 MHz. This provides the performance headroom needed to ensure that card suppliers' investments in software development could be deployed across a wide range of current and future systems.

"The Chip Card industry seeks to provide systems supporting robust and secure high-performance applications in the fast growing financial services and mobile communications markets. These performance requirements surpass the capability of current 16-bit architecture products," said Dr. Hermann Eul, senior vice president and general manager of the Security and Chip Card IC Business Group of Infineon Technologies. "Building on the advantages of our unique system-on-chip design capability and efficient manufacturing processes, we are able to deliver true 32-bit performance and on-chip memory exceeding competitive offerings, at just a small cost premium compared to 16-bit alternatives."

The 88 Family is based on workstation-like core architecture, incorporating on-chip data and instruction caches to support fast program execution by pre-fetching

instructions. It accelerates all Virtual Machine-based Chip Card languages, including JavaSC, MultOS and Windows Powered Smart Cards (WPSC). The chip architecture is also optimized to run multiple tasks in parallel, including peripheral functions such as external communications through the on-chip UART and execution of data encryption and security functions.

To meet requirements for the highest possible security, the 88 Family's integral security concept combines multiple levels of physical protection and encryption support, including the industry's strongest DPA/SPA (Differential Power Analysis/Simple Power Analysis) countermeasures.

The on-chip Memory Management Unit (MMU) incorporates hardware firewalls to isolate and protect applet code from other system elements. In order to support symmetric and asymmetric algorithms, the controller features powerful crypto coprocessors with the highest performance for DES (Data Encryption Standard), Triple-DES, RSA (Rivest, Shamir, Adleman) and elliptic curves algorithms. RSA algorithms with key lengths of 1.024bits are processed in 65 milliseconds without Chinese Remainder Theorem (CRT).

To reduce card suppliers' development costs and speed time-to-market, Infineon also provides a Platform Support Layer (PSL), which is a complete set of low-level drivers for all peripherals and a crypto library for RSA, elliptic curves and AES (Advanced Encryption Standard).

Additional members of the 88 Family will be announced in 2002.

All trademarks are the property of their respective owners.

Open. Independent. Free.

By ACG AG

flashCOS® sets New Standard for Smart Card Operating System



Leading market researchers currently expect a great future for the Smart Card and indeed, the figures seem to back that analysis. With an annual growth rate of almost 40 percent the Smart Card market could be considered one of the most dynamic high-tech markets worldwide. Another growth market - albeit in a more moderate way - will be the SIM-card segment for mobile communication. Datamonitor expects the microprocessor card, which is the central part of a mobile phone, to grow by 21 percent until 2006.

The studies, however, point out than certain restrictions could still hold back the global success of the Smart Card.



New Markets – New Developments

Market analysts have identified the limited storage capacity of the micro-processor card, the still poor security standards and the lack of interoperability among the existing Smart Card systems as some of the obstacles for greater (present) growth. So far, the market is still dominated by proprietary operating systems and the cards can therefore only be used for specific applications.

The resulting dominating position of the proprietary systems of the big players within the Smart Card market is not without problems. Quite a few independent small and medium-sized card manufacturers are very active in this field as well. The latter don't have their own operating systems – especially with development costs that could easily amount to figures around the one million Euro level. Such development costs can only be recovered with a high production volume, a condition which is rarely met by smaller companies. By using the competition's proprietary systems the independent card manufacturers and system integrators don't just back up their own competition – they make themselves dependent on them.

Microprocessors for Smart Cards are mostly dedicated towards the operating systems of one of the big card manufacturers and contain ROM technology. "If you are a small or medium sized card manufacturer – small means a volume of 50,000 to 100,000 cards – and you are going to develop an application for such an operating system, you will have a big problem to solve" says Olaf Jacobi, chairman of the Smart Card business unit at ACG AG. "On one hand you risk that the big manufacturer regards you as a competitor and won't be

forthcoming with any information, on the other hand it wouldn't be in your best interest either, to give them much information regarding your own developments."

In the end, the card manufacturers will have to develop their own operating system, an involved and usually non-profitable procedure, as the development costs are unlikely to pay off. It is this very problem that ACG AG intends to solve.

Flexible Functions

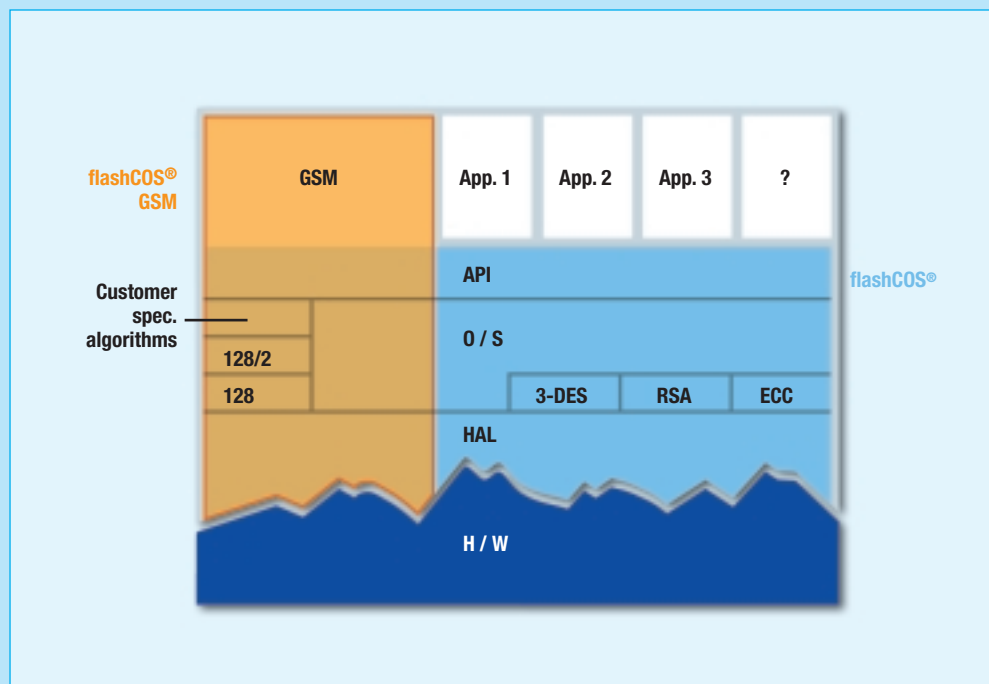
The Danish company **Logos Smart Card A/S**, a subsidiary of ACG AG, solved the problem by developing an operating system that is:

- ▶ Totally self-sufficient and not dependent upon any semiconductor producer or card manufacturer.
- ▶ Available across all hardware platforms
- ▶ And available free of charge as flashCOS® API (Application Programming Interface).

It can be used for almost any Smart Card application as an operating system and is based on the widely used programming language C. Any application-specific software written in C can be run under flashCOS, meaning that the functions of the operating system can be extended and new interface commands can be added. It is also possible to overwrite existing information and create new functions. In this way, flashCOS can be customized to meet the requirements of almost any already-existing Smart Card application.

Modular Software Concept

The core of this concept is a 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, which runs on ROM as well as with flash hardware. To this end, flashCOS is available as both a flash and a ROM version. However, the advantage of flash over ROM technology is the increased hardware efficiency. A 16 KB flash product offers a 32 KB ROM functionality. With ROM, the chip production follows development, however, with flash tech-



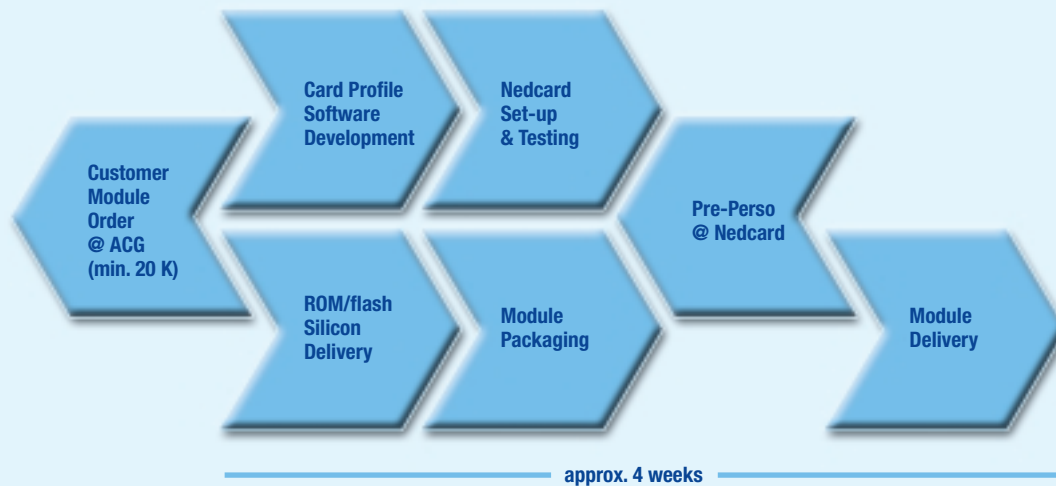


Product Overview

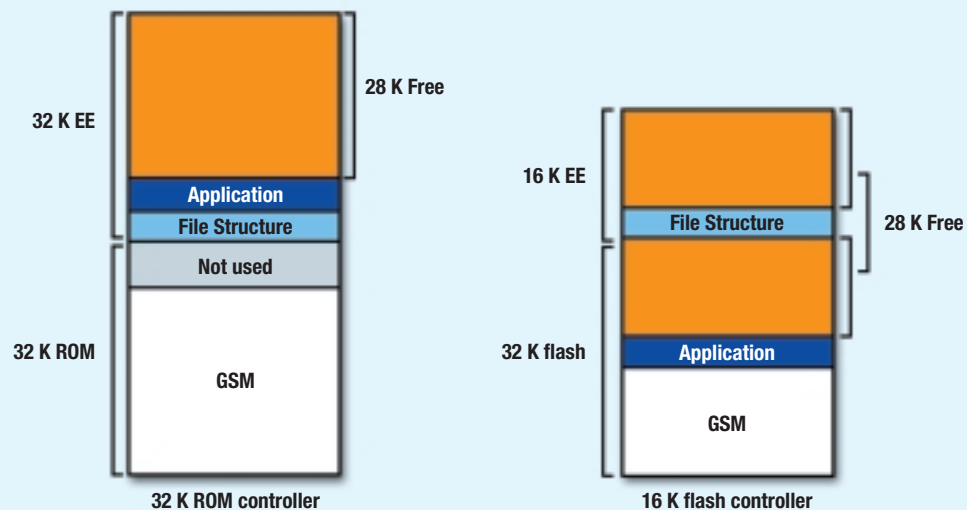
Derivative flashCOS® GSM already Available

Software used to be tied to one or few specific microcontrollers. Not so, with flashCOS® GSM – a truly portable software, which will work with a wide range of microcontrollers. Card manufacturers no longer need to worry about the type of chip.

There is also no development risk or investment in long-term pay-offs: flashCOS® GSM secures a fully operational product with the application that the customer will need – with a minimized lead-time.



The flashCOS® GSM allows the user to personalize the software in line with the chip embedding, as most of the code is loaded already when delivered to the customer.



The advantage of flash over ROM is the increased hardware efficiency. A 16KB flashCOS product offers a 32 KB ROM functionality.



nology, production and development are performed in parallel, with the software written onto the finished module. The modularity of flashCOS is based on open standards and allows the compiler-backed development of applications directly onto the PC without any specialist knowledge of the hardware.

High Security Standard

With regard to any security aspects, flashCOS offers a command and response encryption, a secure file system as well as DES, 3DES, MD2, RSA and ECC security function libraries. These can only be read, written or otherwise changed if both the card reader and the user own precisely defined access rights. This prevents unauthorized access to files on the card. The flashCOS can be used as a single or multifunctional card, but only one party controls the card. With the Java version of the operating system, which is currently under development, several independent users can access a card without access to the data of the other parties. This will be available in the second quarter of 2002.

Special Version for the Mobile Phone Market

For the biggest microcontroller market – the mobile phone market, a special derivative version of flashCOS has been developed. The flashCOS GSM covers the low-end phase II market as well as high end markets with PKI requirements. The product range reaches from small memory capacity up to a 128kB EEPROM chip. It also supports dual and triple mode phones (CDMA, TDMA, AMPS).

The flashCOS GSM is available with a variety of standard applications: An API

programming interface, a scripting and byte code interpreter (LScript) – which is more user-friendly and speeds up writing of applications, a Wireless Internet Browser (WIB), or a user localization interface.

Advantage: Pre-Personalization

The flashCOS reduces production costs by approx. 30 percent due to an efficient pre-personalization. Data that would normally be written on the card during the production process will be uploaded by ACG during module production instead. This is extremely cost-effective as personalization at the manufacturer's end is reduced to a few bytes, as opposed to several kBytes in the past. The only data that needs to be uploaded are the user specific details such as keys, PINs and serial numbers. The production costs of a flashCOS based card are therefore not significantly higher than those of an ordinary telephone card.

The flashCOS Community

The generally open character of flashCOS is enhanced by the web-based information platform at:

www.flashCOS.com, where customers can exchange and expand applications. This website is increasingly becoming a meeting point for all users of this open Smart Card operating system.

“Our goal is to realize a web-based community for developers of micro-processor cards,” says Jacobi. “Similar to the Linux concept, they can exchange thoughts and ideas and mutually improve their applications. The developers have easy access to their applications

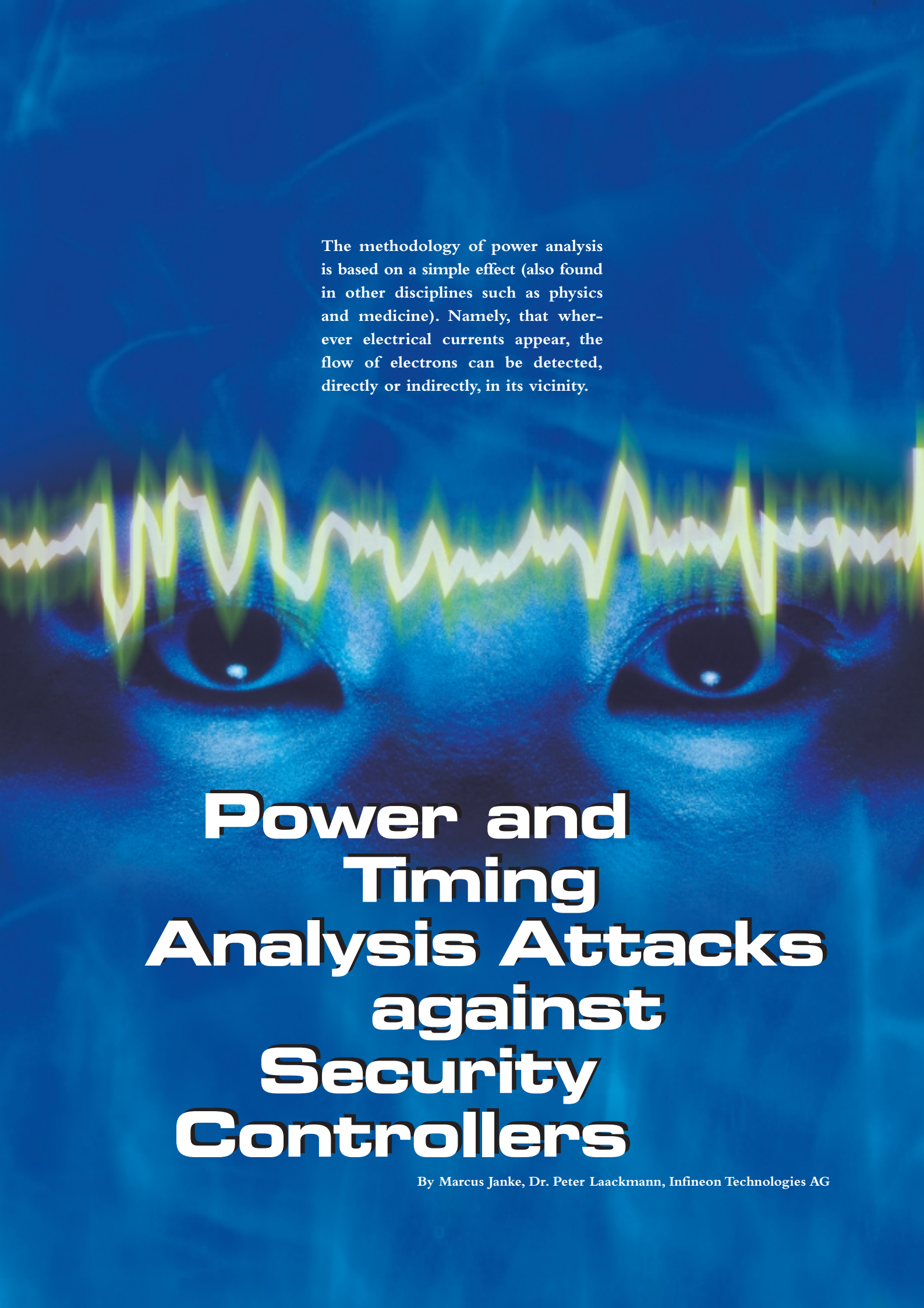
and will be able to customize them according to their individual requirements”. An advantage that will become important for manufacturers of SIM cards as well.

Comparisons to Other Operating Systems

On the SIM card market, Java is currently the only open operating system with a market share of about 8 percent. The open system allows portability of applications, but when it comes to landed-costs and efficiency it will invariably be the most expensive solution on the market. Its memory intensity, too, doesn't speak for Java.

“A flashCOS-application needs only a tenth compared with a Java application with similar functionality”, says Olaf Jacobi. “After Microsoft backed out, Java has practically a monopoly within the market”. An additional option is MultOS, an operating system customized for financial applications. It is believed to be very secure, but never had a decisive breakthrough, primarily because it is based on semiconductors causing considerable operating costs and the proprietor – MasterCard – is in competition with other card issuers.

About 6 Million issues of flashCOS have been sold, which means that MultOS was surpassed in only 12 months. By 2004 ACG plans to hold a market share of 10 percent – an ambitious goal which seems, however, realistic to Jacobi regarding the obvious advantages: “flashCOS GSM is an alternative to Java and MultOS for all SIM applications. The standard version flashCOS is extremely user friendly and keeps the card production costs down as well”.



The methodology of power analysis is based on a simple effect (also found in other disciplines such as physics and medicine). Namely, that wherever electrical currents appear, the flow of electrons can be detected, directly or indirectly, in its vicinity.

Power and Timing Analysis Attacks against Security Controllers

By Marcus Janke, Dr. Peter Laackmann, Infineon Technologies AG

In 1928, the German psychiatrist, Hans Berger, conducted an experiment, which astonished both experts, and laymen – electrodes on a patient's head, connected to an amplifier, could be used to detect the electrical activities of the human brain. The first electroencephalogram (EEG) had been recorded (see Figure 1).

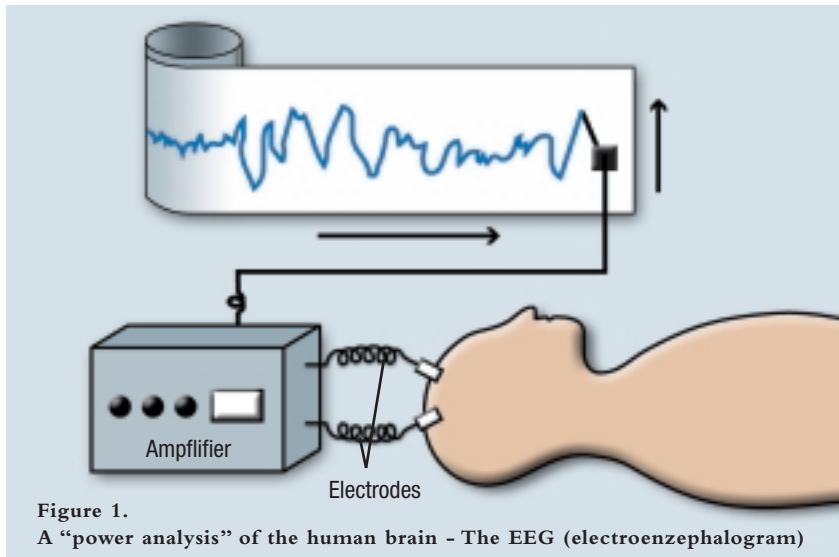


Figure 1.
A “power analysis” of the human brain - The EEG (electroencephalogram)

Berger showed that specific modes (sleep, tranquility, mental stress) could be assigned to specific patterns of EEG signals. Disenchantment was to follow, however, as there began rising panic within the general public as a whole, about the use of EEG technology being used to read the minds of every citizen. There was, in reality, very little cause for concern as experts found out that the immense variety and diversity of weak currents in the brain could only be detected as a sum of all these currents, and could not deliver any information about actual thoughts or single processes in the brain.

The development of power analysis attacks against microcontrollers took a very similar route. For over 50 years it has been commonly known that electronic devices may provide information about their mode of operation through side channels, e.g. their power consumption. A microcontroller in idle mode may only consume a small fraction of the energy that is drawn in active state. Also, there may be variances

in the power consumption that depend on the software code running on such a processor, even depending on the actual command. These effects are mainly based on the number of active switching elements in each state. Standard microcontrollers may also show differences in the power consumption depending on the so called “hamming

weight”, which is defined as the ratio of “ones” and “zeroes” being processed at one time in a register.

If microcontrollers are to be used within security relevant applications, like banking, e-commerce, m-commerce, access control, or pay TV, any side channel leakage that leads to recovery of secret information cannot be tolerated.

Simple Power Analysis - SPA

Unsecured systems, which may also include some Smart Card chips, may show mode-dependent power consumption

values [1]. Ernst Bovenlander demonstrated this effect in 1997 on a Chip Card controller calculating a DES (data encryption standard) encryption [2], and identified the 16 rounds of this procedure. One year later, Kocher, Jaffe und Jun defined two basic attack methods on cryptographic microcontrollers: The “Simple Power Analysis (SPA)” [3] is performed by direct recording of the power consumption and the correlation to specific time spots in the program flow (see Figure 2).

For conducting an SPA, the attacker only needs basic cryptanalytic knowledge, but will need exact information about the program flow, which normally includes detailed knowledge concerning the specific program code. Therefore, the code has to be protected from spying by dedicated barriers – which shows that a protection profile for a secure microcontroller has to be designed from an overall integral security concept. Concerning the mathematics, SPA is truly simple – but the effort needed is still high, (in most cases). In an attempt to save both cost and time, an attacker, would chose another effective attack method – the differential power analysis (DPA):

Differential Power Analysis – DPA

DPA is based on the statistical process for extracting secret data [4, 5]. The first experimental “victim” of a DPA attack was the Data Encryption Standard DES.

The power consumption curves of a microcontroller are being recorded several

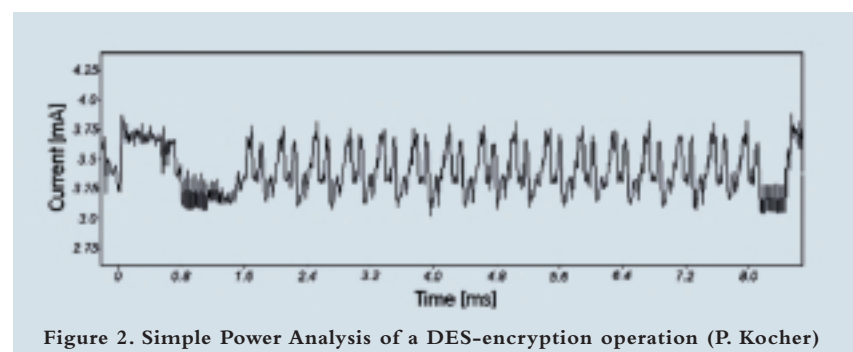


Figure 2. Simple Power Analysis of a DES-encryption operation (P. Kocher)

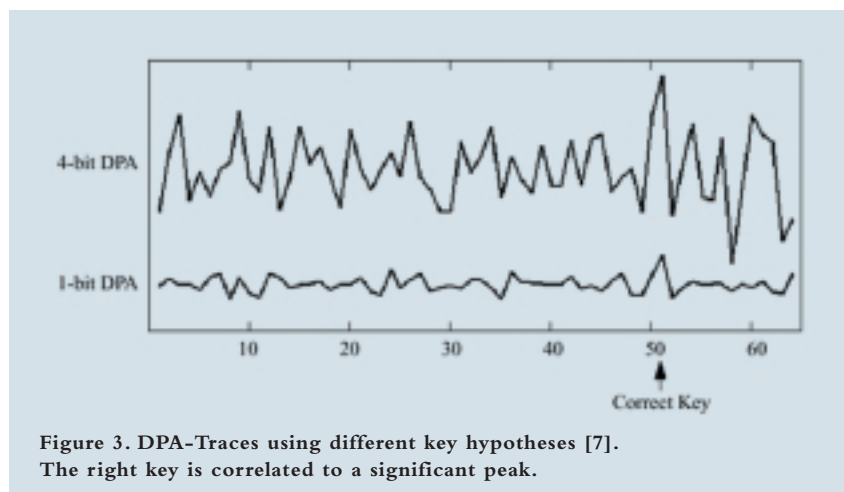


Figure 3. DPA-Traces using different key hypotheses [7].
The right key is correlated to a significant peak.

thousand times. The results are processed using statistical software, dividing the results, sorting them and subsequently storing them in two “stacks”. Then, the trials for the key hypothesis are set up – only the right hypothesis will yield a significant correlation to the power trace. If all trials are displayed in a diagram, the right key will appear as a visible peak (see Figure 3).

Both variants, SPA and DPA, require test equipment which, depending on the difficulty of the attack, ranges from amateur equipment to cost-intensive high professional labs. Due to the fact that nearly all security controllers are equipped with low-frequency detection, a very high scan rate of the SPA/DPA transient recorder is required.

Advanced SPA and DPA Methods

The use of microcontrollers with low power consumption and additional noise generators for power “blurring” pushed the development of advanced

attacks far ahead. The useful information is hidden in a sea of irrelevant but strong noise and has to be extracted by advanced signal analysis methods, consisting mostly of median and filter operations [6, 7] as well as Fourier-transform techniques [8, 9]. In order to strengthen a security microcontroller against these new scenarios, special care is taken to ensure intrinsic security, driven by the design of the cores. These countermeasures act against SPA/DPA attacks by withdrawing the basis of these methods. An integral security concept is absolutely necessary for continued protection.

Timing Attacks

It is not only the power consumption of a microcontroller that may vary with the code sequence and processed datasets. Checking the differences in the processing time may in unsecured systems also retrieve secret information. A comparison to a simple psychological experiment shows the principle of this analysis:

A test person is told to add two numbers. Each individual will use a different amount of time to solve this problem, depending on his mathematical skills and actual condition. Normally, for difficult tasks, more time will be used, but there may be some mathematical tricks, which will shorten the timeframe.

Figure 4 shows the electroencephalogram (EEG) of a test person adding two numbers – producing a mistake – and correcting it subsequently. One may clearly distinguish from the sequences of increased activity that two calculations were performed.

An unsecured microcontroller system, showing data dependencies due to unsecured hardware or software, behaves in a similar way. Addition, Multiplication and Exponentiation may be distinguished, even big values from smaller ones. The same problem arises, if the test of specific values and a following dependant branch in the program code is not secured.

A very simple way of performing a timing analysis attack, developed in the early days of card applications, was to measure the time consumed by a Smart Card to give an answer to an authentication challenge. The attack programs “TimeIt” and “SigPro” used this test for some pay-TV Smart Cards (see Figure 5). If the answer was transmitted significantly faster than the average response time, a valid key was found. These very simple attacks are well known; therefore today’s pay-TV cards are well secured against these kinds of checks.

Timing attacks have been greatly augmented in the last few years. In June 1998, a timing attack could be performed on a Chip Card, compromising

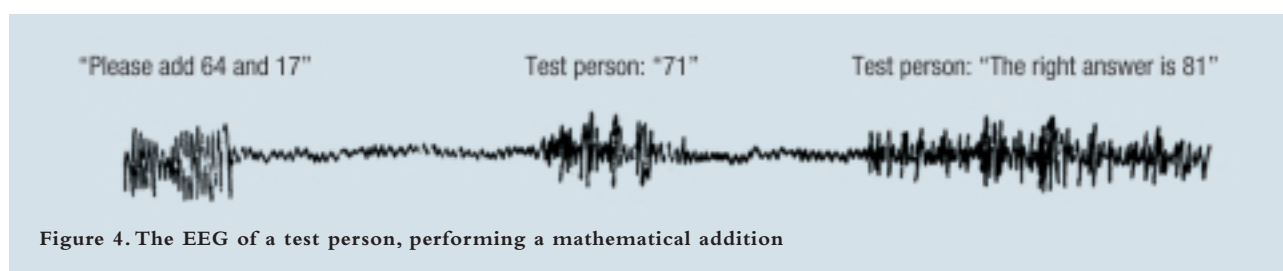


Figure 4. The EEG of a test person, performing a mathematical addition



a software test code for the RSA public key cryptography. After analyzing 300,000 timing tests, a 512-bit RSA key could be determined. The overall time for this attack has been specified to only a few minutes [10]. In this study, the individual bits of the RSA key were tested sequentially. It is important to know that this specific kind of attack worked only for the conventional RSA method, not for the faster CRT (Chinese Remainder Theorem) variant. The German BSI [11] demonstrated a further evolution of this method, breaking the barriers of the RSA-CRT applications. The attack can only be effectively performed if the so-called “Montgomery Algorithm” is used for calculation of the RSA, and if the Chinese Remainder Theorem (CRT) is used.

secure microcontrollers from Infineon Technologies are equipped with high-performance, hardware based, countermeasures that assist the software in an optimal way to reach the target of high system security.

Electromagnetic Emanation Analysis - EMA

Due to the very nature of electrons, every little electrical current in a copper wire, electrical component or microchip will induce magnetic fields. If the electrical current stays constant, a static magnetic field is observed. Changes in the current will produce alternating magnetic fields – and any sudden changes lead to detectable electromagnetic fields that may easily be detected in the vicinity. Therefore, a

enciphered transmission – meaning the device could be broken. Furthermore, a review article from 1986 refers to sources dating back to 1967 [13]. The conclusion: that unsecured Smart Card controllers could be compromised by similar attacks, has also been published in reports as early as 1994[14, 15].

As the electromagnetic emanations of a microcontroller may include the whole chip (not only the power supply lines), it is obvious, that simple countermeasures against SPA/DPA will not provide complete protection. If the design of a microcontroller is not intrinsically secured (which means preventing the origin of electromagnetic emanations), an EMA attack could be considered as a real possibility. Therefore, special design features and a sophisticated architecture providing integral security

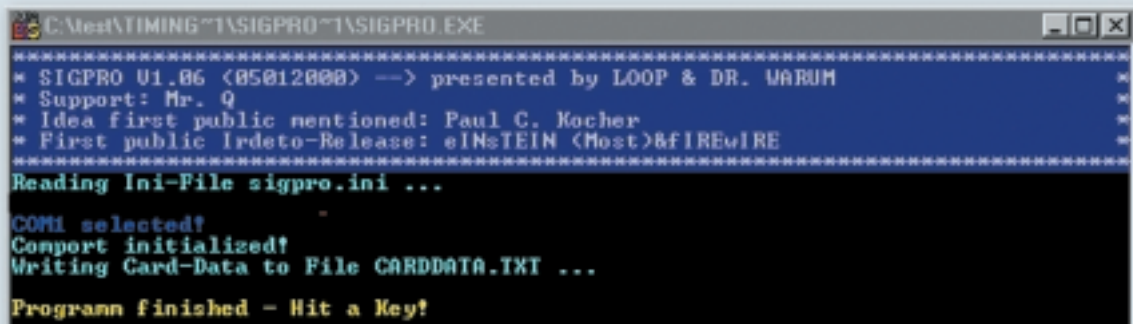


Figure 5. “SigPro” - One of the first practical timing attacks

Timing analysis attacks and power analysis attacks (SPA and DPA) have a very close relationship with each other. If a microcontroller is insufficiently protected against power analysis, further information about time dependencies may leak through these side channels – for example, an attacker may measure timing values between significant power profiles.

Countermeasures against these attacks will, in every case, combine software and hardware features. Software has to be tuned to the specific hardware and vice versa. All algorithms and program code slices, which are of relevance concerning security, have to be designed as time-neutral, so that no information may be gained about possible secret data. To provide further security, the

simple coil can be applied, surrounding the device to be tested. Static fields are detected using semiconductor “hall sensors” or “SQUIDS” (superconducting quantum interference devices) at low temperatures. Whereas the static fields only play an insignificant role in the attack scenarios, the emanation of alternating electromagnetic fields is well known for discovering secrets via side channels. A practical attack was performed in 1960; described in an autobiography written by the former MI5-scientist Peter Wright [12]. The input terminal of a cryptographic Teletype device generated very strong signals, which were propagated in clear text through the entire machine. Using an appropriate amplifier, the weak clear text signals could be separated from the

is an important base for systems providing security. Both for today and for the future.

The first public EMA attacks on single chip microcontrollers [16] targeted the emanation spectrum of commonly used microcontrollers, not Smart Card variants. Industrial research today goes one step further, using dedicated equipment for evaluating EMA attacks on Smart Card controllers [17].

Evaluation and Development of Power and Timing Analysis Methodology at Infineon Technologies

Power analysis has been one of the central points of security efforts in the last



years of Smart Card security research and discussion, including hardware, software and application/system knowledge. Infineon Technologies has been, in the last few years, thoroughly evaluating these attack scenarios so that the new requirements, especially in the field of certification, could be instantly

fulfilled. Looking far ahead is a fundamental principle of tomorrow's Smart Card security [18]. The development of new products is oriented not only on today's requirements: possible attack technologies of the next few years are already tested today, leading to own evaluation capabilities and test platforms for

the new generation of power analysis attacks. One way for achieving this task is to use the latest devices for digital signal processing, combined with sophisticated analysis software developed by cryptologists, mathematicians, attack specialists and test engineers, working in close cooperation.

Literature

- [1] J. L. Zoreda, J. M. Oton, "Smart Cards", Artech House, **1994**.
- [2] E. Bovenlander, "Invited Talk on Smartcard Security", Eurocrypt Konstanz, **1997**.
- [3] P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", Cryptographic Research, Inc., San Francisco **1998**.
- [4] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", Proceedings Advances in Cryptology - CRYPTO99, Springer Verlag **1999**, 388-297.
- [5] J.-S. Coron, P. Kocher, D. Naccache, "Statistics and Secret Leakage", Ecole Normale Supérieure, Paris; Cryptography Research Inc., San Francisco; Gemplus Card International, Issy-les-Moulineaux, **2000**.
- [6] 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", Worcester, USA **2000**.
- [7] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards", USENIX Workshop on Smartcard Technology, Chicago, **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", Worcester, USA **2000**.
- [9] D. Naccache, F. Olivier, "Blind Deconvolution and DPA Resynchronization", Presentation "CHES 2000, Workshop on Cryptographic Hardware and Embedded Systems", Worcester, USA **2000**.
- [10] J. F. Dhem, F. Koeune, P.A. Leroux, P. Mestre, J. J. Quisquater, J. L. Willems, "A Practical Implementation of the Timing Attack", UCL Crypto Group Technical Report CG-1998/1, UCL Université Catholique de Louvain, **1998**.
- [11] W. Schindler, "A Timing Attack against RSA with the Chinese Remainder Theorem", Presentation "CHES 2000, Workshop on Cryptographic Hardware and Embedded Systems", Worcester, USA **2000**.
- [12] P. Wright, "Spycatcher - The Candid Autobiography of a Senior Intelligence Officer", William Heinemann, Australia **1987**.
- [13] H. J. Highland, "Electromagnetic Radiation Revisited", Computers and Security **5**, **1986**, 85-93.
- [14] J. Szigals, "Smartcards - A Security Assessment", Computer and Security, Elsevier Science **13**, **1994**, 107-114.
- [15] M. C. Kang, "Smartcard Based System is Inherently Insecure", 07.07.1996.
- [16] Markus G. Kuhn, in Antoveldre, "Markus Kuhn Annabteada", Newsgroup "ee.arvutid.turvalisus", 23rd November **1999**.
- [17] K. Gandolfi, C. Mourtel, F. Olivier, "Electromagnetic Analysis: Concrete Results", in C. K. Koc, D. Naccache, C. Paar (eds.), "Proceedings Cryptographic Hardware and Embedded Systems CHES 2001", Paris **2001**.
- [18] P. Laackmann, "Mit Sicherheit gute Karten - Transparente Kryptographie: Neue Herausforderungen für Chipkarten-Entwickler", Elektronik **23**, **2000**, 78-80.

BIOMETRICS BUSINESS AND SECURITY 2002

Conrad Hotel, Brussels, Belgium
9-10 April 2002

Biometric technologies are emerging as a major tool for companies seeking maximum security and convenience – find out how developments in the biometric industry can improve levels of security, quality of customer service and increase cost-effectiveness for your organisation.

At **Biometrics: Business and Security 2002** a top quality list of invited speakers will focus on real-life case studies, technological developments and practical applications in the three hottest application areas in the industry today – the law and order, financial services and travel sectors. In addition, a long line-up of speakers will address the crucial wider issues facing the industry together with an update on all the cutting edge technological developments.

Organised by:



Programme sponsor:



Hear from visionary keynote speakers and leading users of biometric systems in the following industries

Biometrics in Financial Services

From e-banking to secure financial document exchange, biometric technology has the potential to revolutionize the way the financial services industry operates. This stream will address all the major issues facing financial institutions with regards to authentication, both in the virtual and customer facing environment.

Opportunities for Biometrics in Law and Order

The use of biometrics for street surveillance, national ID cards, tracking inmates, identifying sexually abused children and even in the production of a smart gun are all active areas of interest. The expert speakers in this stream will bring together all these developments and provide insight into possible future applications.

What Biometrics has to Offer the Travel Industry

This stream will bring to light exactly what can and can't be achieved with biometric technology. As well as speeches from industry leaders on issues such as rebuilding passenger trust, there will be numerous informative case studies, looking both at passenger processing and convenience as well as practical advice on how to enhance airport security.

Progress in Biometric Technologies and Management Issues

With presentations looking at market reviews, advice on integration, privacy concerns, technology selection, standards and the biometric "business case" among others, this stream will be of interest to everyone using or considering the use of biometric technologies.

For full programme details visit the conference website at:

www.biometricseurope2002.com

or contact a.williams@elsevier.co.uk

Tel: +44 (0) 1865 843089

www.biometricseurope2002.com

Biometric System Security

By Colin Soutar, Bioscrypt Inc.



Unauthorized User!
Access denied!



The availability of the biometric application programming interface, BioAPI, has facilitated the integration of biometric systems into applications. One of the important considerations in the definition of the API was to identify and prevent any potential security attacks that could arise as a result of its usage. This article describes how a particular attack, known as the “hill-climbing” attack, was identified and resolved during the development of BioAPI.

Historically the integration of biometric technologies into applications was achieved using proprietary software developers' kits (SDK's). More recently, a standardized biometric application programming interface BioAPI, (version 1.1 of the specification was released in March 2001) was defined to facilitate the portability of different biometric technologies within applications. As such interfaces are developed, there is an increasing awareness of security risks associated with information passed between the biometric technology and the PC application. The development of open standardized function calls to the biometric technology, creates the possibility that “rogue” applications can be written to mimic the actions of a legitimate application and thus compromise security of the system. This article discusses the particular issue of passing authentication scores from the biometric technology to the application, and provides a method to eliminate the security risk associated with this action.

Statement of problem

Figure 1 presents the basic processes for authentication of a biometric sample. The biometric sample is compared with a template within the Biometric Service Provider (BSP) to create a score. This score is then compared with a pre-defined threshold and the person who provided the sample is either authorized as the legitimate holder of the template or not. The release of scores

from the BSP to the application becomes a security issue when passed through open standardized means (such as an API). In this case, an attacker can write a rogue application that systematically interrogates a BSP by providing a sample that is randomly perturbed and monitoring the output score to maintain only changes in the sample that move it closer to the image represented by the template. The attacker can thus systematically modify the sample to obtain progressively higher scores until the decision threshold is met. Such an attack can be labeled a “hill-climbing” attack (see Figure 2).

To demonstrate the vulnerability of biometric (and other pattern recognition) systems to the hill-climbing attack, a simplified pattern recognition system was simulated using the two images shown in Figure 3 with a generic phase-only filter based correlator, such as that described in U.S. patent 5,214,534, by Kallman et al. Filters were first created using both the space shuttle and the Apache

helicopter images and these filters were then matched with both input samples to obtain the scores given in the table.

On the basis of the table of scores (next page), a pattern recognition system can be set up to discriminate the two objects, using a decision threshold of ~ 50 . To demonstrate the hill-climbing attack, a filter was constructed using the space shuttle image and the Apache image was used as the input sample. At each iteration of the simulation, a certain number of pixels within the input sample were randomly modified (pixels at random locations were set to a random value between 0 and 255). At each iteration of the simulation, the output score was examined, as presented in Figure 2, and only sets of modified pixel values that contributed positively to the score were maintained. We determined that the optimal number of pixels (for efficiency) to modify per iteration was 64.

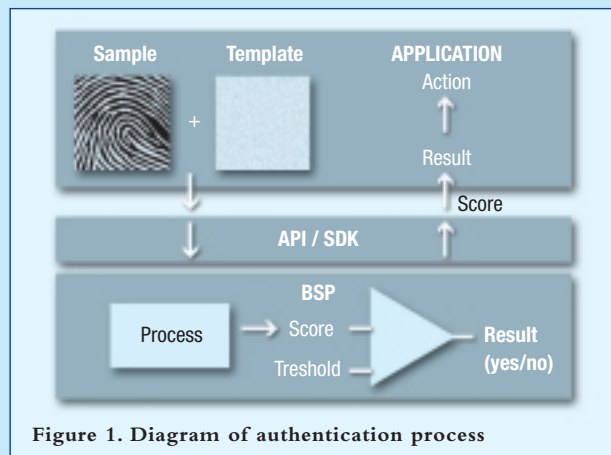


Figure 1. Diagram of authentication process

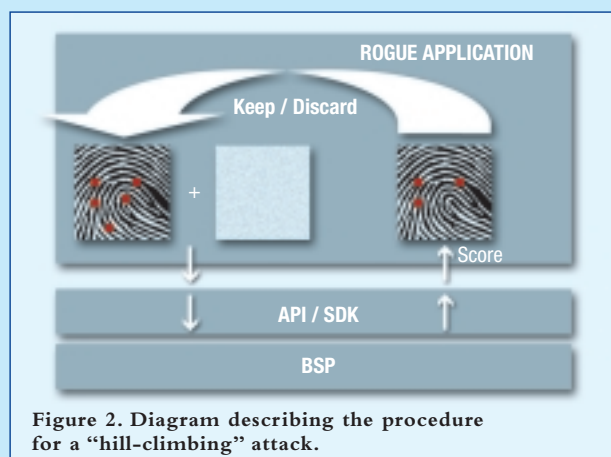


Figure 2. Diagram describing the procedure for a “hill-climbing” attack.



Figure 3. Space shuttle and Apache helicopter images

filter Input sample	Shuttle	Apache
Shuttle	933	0.463
Apache	0.329	242

Figure 4 presents the progression of scores as a function of iteration. Note that the score of 50 that was proposed as the threshold is fairly easily achieved (after about 600 iterations). The modified Apache sample at this point would be capable of being erroneously recognized as the space shuttle.

The simulation continued to run for several days, to produce the image shown in Figure 5, after 7 million iterations.

Note that the outline of the shuttle is evident, as expected with a phase-only filter.

Solution

To understand the solution to the hill-climbing issue, it is instructive to examine the probability of attaining scores based on the process of randomly changing pixel values. To model this, we established an input sample that produced a score of 25 (selected to be midway between 0 and 50, the decision threshold). For a number of instances (20,000) a set of 64 pixels was randomly modified, as previously described, and the resulting score was logged. The

set of these data is presented as the histogram shown in Figure 6. Note that the distribution is approximately symmetric around 25. Therefore, an attacker with access to these scores can easily determine which changes in the input sample to maintain (based on the changes that increase the score). Note however, that the number of occurrences of jumping from 25 to higher values becomes diminishingly small. Therefore, if we only allow the return of a score once it has surpassed a specified increment, then the probability of a random perturbation creating such a jump becomes very small. Indeed, we can plot the probability of jumping from 25 to a particular score, as presented in Figure 7, by integrating under the distribution shown in Figure 6.

Based on the probability distribution of Figure 7, we see that the probability of producing a score of (say) 27.5, starting from 25, is very small. Thus, we stipulate that scores can only be transmitted from the biometric system to the application in quantized levels, say in steps of 2.5 for this particular case, then a potential attacker can only know if a random fluctuation was successful in a very small number of cases. In other words, if the input sample produces a score of 25, then the probability of producing a score of 27.5 or higher and so

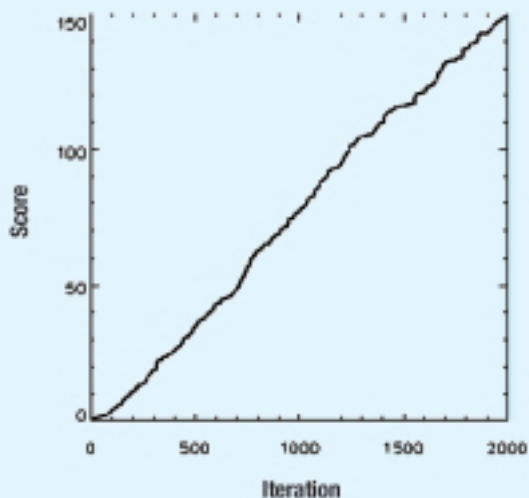


Figure 4. Progression of score as a function of iteration



Figure 5. Input sample after 7 million iterations

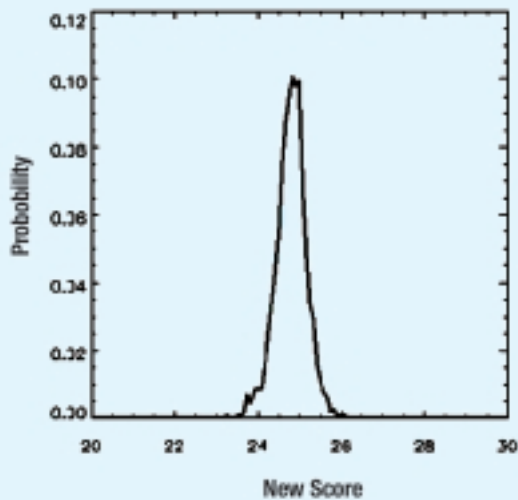


Figure 6. Probability of attaining score

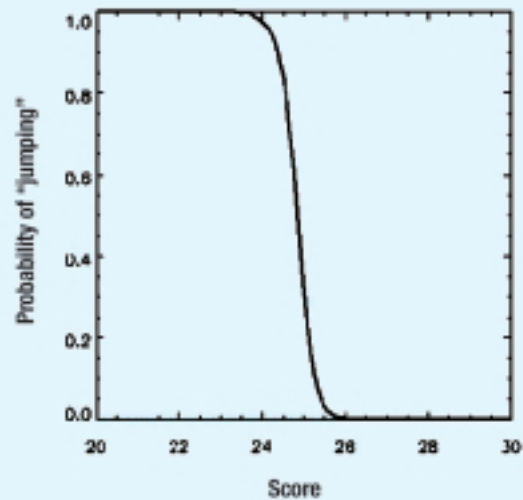


Figure 7. Probability of "jumping" from 25

being released by the BSP is very small, as given by the plot in Figure 7. Placing such a limitation in the system and running the simulation again produces the data shown in Figure 8.

This plot should be compared with the plot in Figure 4. Note that in this case the hill-climbing process is very much slower. Indeed, linear extrapolation of the plot indicates that the threshold score of 50 would only be attained after 10^{16} iterations. This makes such an attack prohibitively time-consuming.

The steps of 2.5 were chosen as an example only and can easily be expanded, to make such an attack even more difficult. Figure 9 presents the input sample that is obtained after these 7 million iterations. Note that the input sample still resembles the original Apache image. Note that the quantization level of 2.5 was chosen for illustrative purposes only, and the level of quantization required for a biometric system should be carefully chosen based on the biometric type and the form of the recognition system. This phase-only

based correlation system presented here was chosen as one that is particularly susceptible to this issue, again for illustrative purposes.

Conclusions

We have presented a method to eliminate the hill-climbing attack on a biometric system, by limiting the precision of scores returned from the biometric system to the application. The use of this method is recommended in the BioAPI specification as an appropriate way to eliminate hill-climbing attacks.

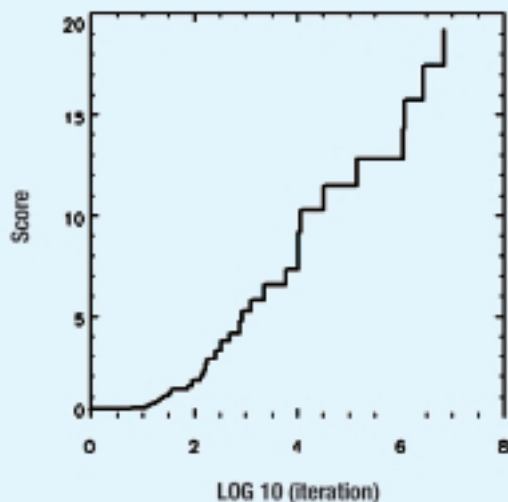


Figure 8. Progression of the score as a function of LOG10 (iterations)



Figure 9. Modified Apache image



Improving Biometrics

By Dr. Susan Thompson,
Datacard Consult p7



We are frequently seeing biometrics proposed as solutions to identification problems in commercial and government applications – especially those associated with international border control and welfare payments. In the UK alone financial losses in this latter area due to mistaken identity are believed to be measured in billions of pounds annually. Unlike its PIN and ATM card counterparts, a biometric has the advantage of being non-transferable. But in the past the use of biometrics has been stymied by the demands of the technologies involved, cost and large, variable user populations. It is partly for this reason that deployment of biometrics has been patchy. This is now changing. Recent progress in biometrics suggests that performance accuracy can be improved in a number of ways. We consider how.

Biometrics Overview

Biometric applications are used to authenticate user access to a computer system by means of some physical or behavioral characteristic that is unique to each individual, e.g. face, voice, fingerprint, gait, scent, DNA. To use such an application, individuals must first enroll by submitting samples of their biometric. These are used to form a template that is stored locally or remotely and used in subsequent pattern matching. A typical system overview is depicted in *Figure 1*.

Biometric applications are of two types – ID and verification. When a user logs on to an ID application the biometric generated by the user is used to identify the user from a database of user templates, i.e. a large number of comparisons are needed. In a verification application the user will already have chosen an identity.

The template corresponding to that identity is selected from the database and matched with that generated by the user, i.e. a single comparison. Because biometrics are vulnerable to measurement inaccuracies, each comparison produces a score that is compared with a threshold. If this comparison is favorable, the match is accepted.

The verification application is a direct one-to-one comparison. In this case improvement in the accuracy of the biometric is usually sought. For example, the threshold value is critical: too lenient and there will be many false matches, too harsh and genuine matches may fail. Selection of an appropriate threshold will ultimately depend upon the requirements of the system and the limitations of the biometric measure.

Clearly, the ID application is the more

demanding, as it requires many more comparisons. Improvements in the performance of the biometric with respect to both time and accuracy are important in this case. This will also depend upon the way the template database is organized and its size.

Evaluating a Biometric

Common approaches to evaluating the performance of a biometric system are based upon the following criteria:

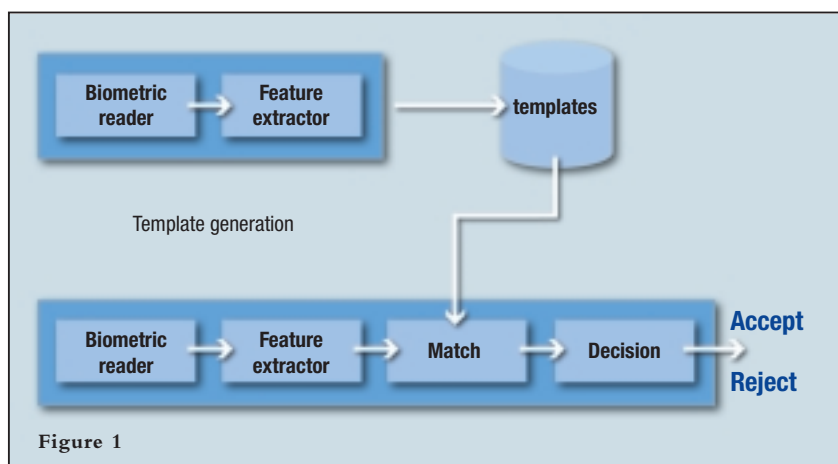
- ▶ Frequency Distributions of biometric scores
- ▶ Failure to acquire (FTA)
- ▶ Failure to enroll (FTE)

Others, such as cost, throughput and susceptibility to environmental factors are not considered here. Instead we provide a limited basis for assessment of a proposed biometric, prior to use in a system.

Other criteria associated with evaluating biometrics, e.g. optimizing database search in ID applications, are discussed in [3].

Frequency Distributions

The generation of biometric frequency distributions is a slightly thorny issue. In practice it is difficult to obtain unbiased samples of the end users. Hence, for this discussion it is assumed that testing is on a representative sample of end users and that the biometric data is appropriate for the analysis below.



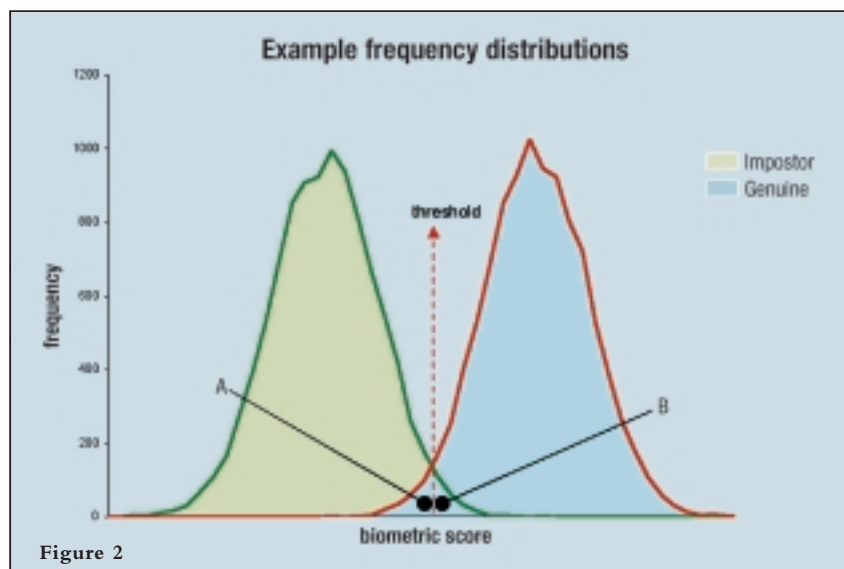


Figure 2

There are two frequency distributions to consider when evaluating a biometric, the distribution of values of the biometric measure when the user is

- ▶ genuine
- ▶ an impostor

The a priori distributions are unlikely to be available for such investigations. Furthermore, it is generally difficult to obtain the large samples necessary to characterize such distributions – in particular, the conditions under which trial distributions are obtained may be significantly different from conditions where the biometric will be applied in practice.

It is assumed here that the distributions are Normal although this may not be the

case in practice. Two (simulated) example distributions are shown in Figure 2. Each plot represents the distribution of 10,000 biometric scores.

FAR/FRR/EER

The regions A and B represent the uncertainty of the biometric. These are where the two frequency distributions overlap so that unequivocal selection of the original distribution given the value of the biometric is impossible. A “perfect” biometric measure, i.e. one allowing perfect discrimination between an impostor and a genuine user, will have no such region.

A biometric is often described in terms of its false acceptance rate (FAR) and

false rejection rate (FRR). Briefly, a biometric returns 4 possible results:

- ▶ Acceptance when user is genuine
- ▶ Rejection when user is genuine (False Rejection)
- ▶ Acceptance when user is an impostor (False Acceptance)
- ▶ Rejection when user is an impostor

Assume a threshold value for the biometric as indicated on the graph left. Rejecting values of the biometric less than this threshold will result in false rejection of the proportion of genuine users represented by region A.

Accepting values of the biometric in excess of the threshold will result in false acceptance of the proportion of impostors represented by region B. Hence, region A represents the FRR and region B represents the FAR for the biometric at this particular threshold (and under the test conditions).

It can be seen that increasing or reducing the threshold has an impact on the FRR/FAR with one decreasing at the expense of the other. The equal error rate (EER) is at the threshold where $FAR = FRR$. This case is depicted in the graph above. A low EER is desirable as this suggests better separation of the impostor/genuine user frequency distributions.

The requirement to minimize one error rate at the expense of the other depends largely upon the application.

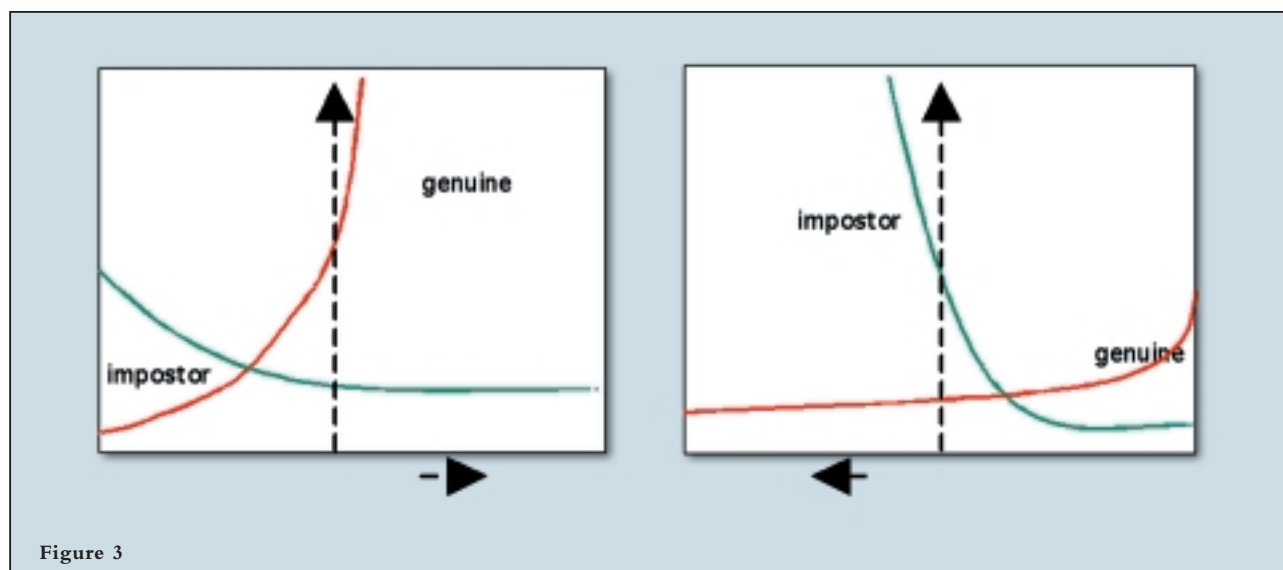


Figure 3



High security applications, e.g. prison, may tolerate a relatively high FAR in order to maintain a low FRR whereas some bank applications may favor the opposite approach. Most commercial applications seek to minimize both.

Other factors that affect the FAR/FRR are the relative shapes of the impostor/genuine frequency distributions – particularly in the region of uncertainty. These will depend upon the biometric measures themselves (and the conditions under which the biometric is collected).

If the genuine user frequency distribution is very steep compared to the impostor distribution in this region then small changes in the FAR may correspond to large changes in the FRR (left Figure 3). For example, increasing the threshold in this case results in a greater proportion of genuine users being rejected by comparison to the number of impostors being accepted.

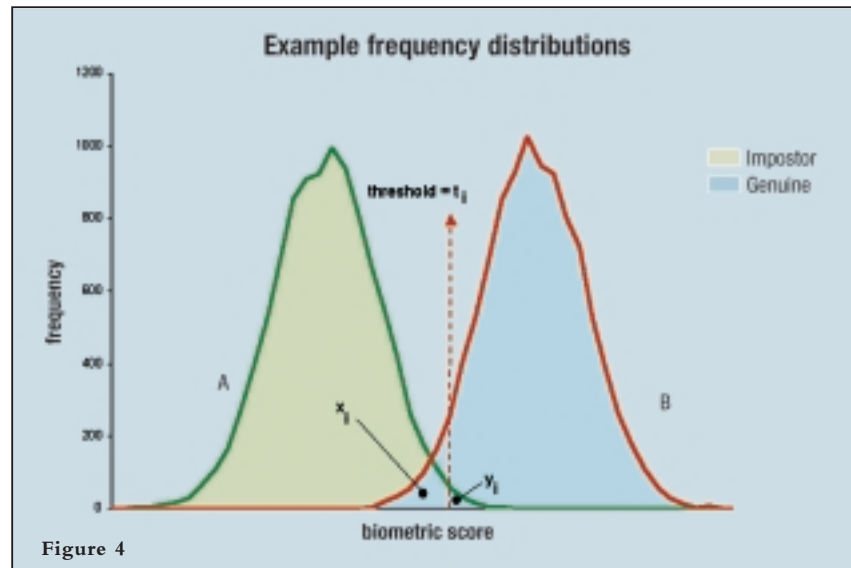
Conversely, a steeper impostor distribution in this area will produce large changes in the FAR corresponding to small changes in the FRR (right Figure 3). For example, decreasing the threshold in this case results in a greater proportion of impostors being accepted by comparison to the number of genuine users being rejected.

From this we can see that it would be very convenient if we could influence these distributions in such a way that the “shape” was more appropriate to the application.

Comparing biometrics

The previous section showed how inspection of the empirical frequency distributions can be a guide to the accuracy of a biometric measure. It is also useful to be able to compare the accuracy of a number of biometrics. Two ways used to compare the effectiveness of a number of biometrics are:

- ▶ The receiver operating characteristic (ROC) chart
- ▶ The separation of the two curves – d' .



ROC chart

The ROC chart shows the inverse relationship between the FRR and FAR.

To generate a ROC chart for a given biometric frequency distribution, plot the set of ordered pairs (x_i, y_i) corresponding to a threshold value t_i in the set $T = \{t_0, t_1, \dots, t_k\}$.

In the example shown in Figure 4, the value of x_i is obtained by integrating under the genuine curve from $-\infty$ to t_i and y_i is obtained by integrating under the impostor curve from t_i to $+\infty$.

In this way it is possible to compare the performance of a number of biometrics with respect to FRR and FAR. Figure 5 shows some possible ROC plots. Points

near the origin minimize the FAR and FRR for a given biometric experiment.

Plots that are symmetric about the EER threshold suggest similar impostor/genuine user distributions. Generally, the more closely the plot follows the xy axis, the better the separation offered by the two distributions, the smaller the FRR/FAR and hence the better the discrimination offered by the biometric. As a rule of thumb a low EER is desirable. The rate of change of each error rate with respect to the other is immediately apparent from this plot. For example Plot (a) depicts a biometric where the FAR is fixed and invariant

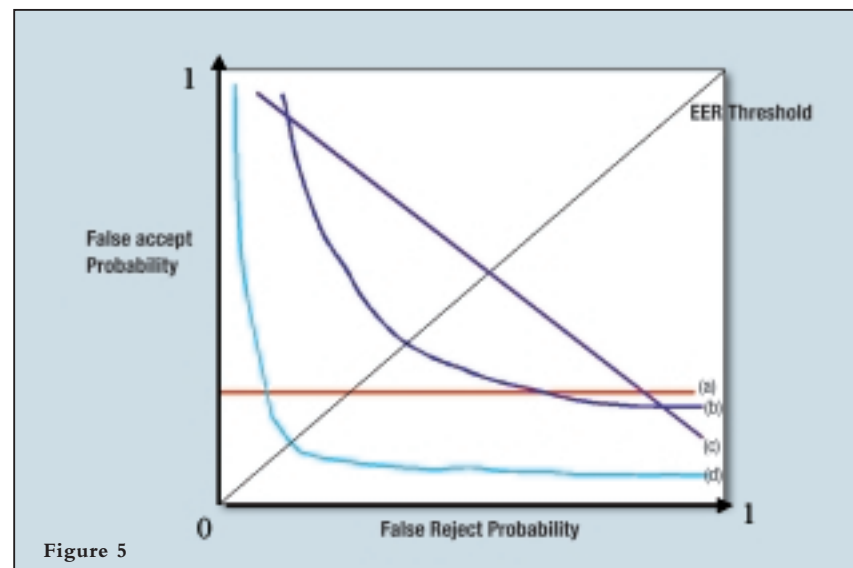


Figure 5



with the FRR. In this case the threshold that minimizes the FRR might be the best option.

In all cases selection of the appropriate threshold will depend upon the application requirements.

Separation of means – d'

If there is a posteriori evidence to suggest that the relevant distributions (impostor, genuine) are Normal, an alternative approach to comparing a number of biometrics is to look at the difference of the two distribution means for each biometric, appropriately scaled, e.g. for each biometric compute $d' = \text{abs} \{ (m_1 - m_2) / \sqrt{[(SD_1^2 + SD_2^2)/2]} \}$ where m_i and SD_i , $i = 1, 2$, denote mean and standard deviation of the impostor and genuine user.

Clearly, larger values for d' suggest better separation and hence better discrimination between impostors and genuine users.

As an example of the usefulness of this statistic assume that the distributions are Normal with a standard deviation of 1. Suppose regions A and B should each comprise 5% of the observations (EER = 5%). This implies $d' = 3.28$. If

A and B should each comprise 1% of the observations (EER = 1%), $f = 4.65$.

Failure to Acquire

A small proportion of a population using a biometric system will be unable to provide a sample that can be analyzed by the system. The proportion of attempts that result in this type of failure is the FTA rate. This may have many causes, e.g. environment, technology, user-friendliness. Clearly, a low FTA rate is desirable.

Failure to Enroll

A small proportion of a population using a biometric system will be unable to provide a reliable template for system matching. This proportion is the FTE rate. Clearly, a low FTE is desirable.

Improving a single biometric system

We have seen how the accuracy of the biometric system may be measured in terms of FAR/FRR/FTA/FTE. To some extent these can be bettered by improving the enrolment and usage conditions. However, it is sometimes possible to do better:

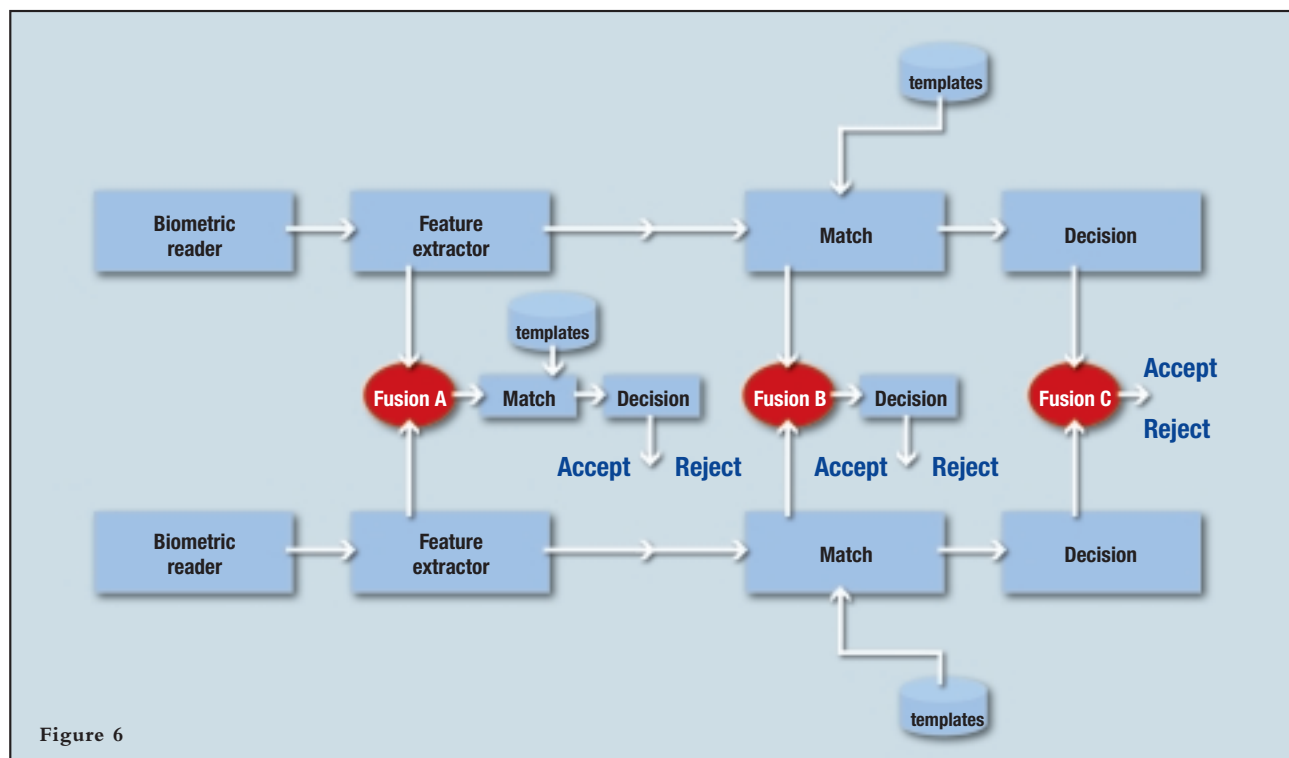
Multiple application of the same biometric with a FAR = 5% and FRR = 1% at a particular threshold. The probability of accepting a genuine user = 99%, the probability of rejecting an impostor = 0.95. Consider a system that permits a user 3 attempts and fails only those users who present 3 failures. The probability that a genuine user will obtain 3 failures is 0.01^3 . So the new FRR = 0.000001, i.e. better than before.

An impostor will be accepted if any of the following occur:

- Pass first time with probability 0.05
- Pass on second attempt with probability $0.95 \times 0.05 = 0.0475$
- Pass on third attempt with probability $0.95^2 \times 0.05 = 0.0451$

This gives a corresponding FAR = $0.05 + 0.0475 + 0.0451 = 0.143$, i.e. worse than before.

If the failure criteria is changed to 1, the corresponding FRR is now 0.0297, i.e. worse than before but the FAR = 0.000125, i.e. better than before. In fact we can tabulate the FRR and FAR as follows.





Fail criteria (Max number of failures out of 3)	New FAR	New FRR
1	0.000125	0.029701
2	0.00725	0.000298
3	0.143	0.000001

We see that there is an improvement in both of the new error rates (in theory at least) when the fail criteria is set to 2. Changing the threshold, and hence the FAR and FRR, will impact these new error rates values further.

- The biometric may be applied with some other form of authentication, say memory-based (PIN) or possession-based (Smart Card).

For example assume a biometric is used in conjunction with a 4 digit PIN, with 1 attempt at the PIN and 1 attempt at the biometric with the same FAR/FRR as defined above. In this case the $FAR = (0.1)^4 \times 0.05 = 0.000005$, $FRR = 0.01$.

- Applying error correction techniques to the template and the sampled biometric in order to improve the match score[10].

Multibiometric systems

We have been considering biometric systems that use a single user characteristic. But in practice, a system relying on a single biometric is often unable to cope with the requirements of accuracy when applied over a large target population. Eventually, even improvements in the technology may not result in much practical improvement in performance.

The main reason for this is that in order to cope with e.g. gender and racial differences, the threshold may have to be fairly lenient. How lenient, of course, is dependent upon the final application. Even so, some users may be unable to provide a biometric at all, e.g. a person without hands cannot produce fingerprints.

It is partly for this reason that multibiometric systems have been considered. Although single biometric systems can be more cost-efficient, the use of multibiometrics may enable more accurate

performance over a larger target population [1]. Improvements in required accuracy may be achieved by using fusion techniques [2] applied at the biometric definition, template matching or end decision levels, as shown in Figure 6.

In the previous section, we saw that three applications of the same biometric can result in error rates (FAR/FRR) that are improved or worsened beyond that of the single application of the biometric. In [7], Daugman makes a similar observation when discussing the combination of two biometrics, where one is stronger than the other. This suggests that indiscriminate combination of biometrics is undesirable.

Furthermore, a glance at Figure 6 shows that the number of possible combinations is non-trivial. In other words, if you have a number of biometrics each with a different ROC it is unclear how to optimally fuse them in a way that best suits the application. For example, do you apply the biometrics in a fixed sequence, each conditional on the last, or apply a majority vote decision to a number of biometrics, or weight the results in some way? You simply have to model the joint distribution determined by the selected fusion technique and compare its performance, using the techniques discussed earlier, with that of the individual biometrics themselves.

In conclusion, for a specific application it may be unclear what biometrics to use, how many to use and how to combine them. Furthermore, some applications may not permit the luxury of many time-consuming biometric comparisons. Nevertheless, evidence [12] suggests that confidence in the use of multibiometrics to address ID and authentication is now well placed with the diversity of biometrics that are currently available to match the application domain. It is likely that we will see increasing reliance on systems that integrate multiple biometrics and other authentication technologies to improve robustness.

References

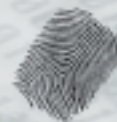
1. "Can Multibiometrics Improve Performance?" Lin Hong, Anil Jain, Sharath Pankanti. *Proceedings AutoID'99*, Summit, NJ, Oct 1999, PP. 59-64.
2. "Information Fusion in Biometrics", Arun Ross, Anil Jain and Jianzhong Qian.
3. "Biometrics: Personal Identification in Networked society", A.K. Jain, R. Bolle and S. Pankanti (eds.), Kluwer Academic Publishers, 1999.
4. Association for Biometrics, <http://www.afib.org.uk>.
5. Biometrics Consortium, <http://www.biometrics.org>.
6. "Decision-Level Fusion in Fingerprint Verification", S. Prabhakar and Anil K. Jain, *Pattern Recognition*, 2001.
7. "Combining Multiple Biometrics", John Daugman, <http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html>.
8. "Best Practices in Testing and Reporting Performance of Biometric Devices", Biometrics Working Group.
9. "Introduction to Evaluating Biometric Systems", P.J. Phillips, A. Martin, C. Wilson, M. Przybocki, *IEEE Computer Magazine*, January 2000.
10. "On Enabling Secure Applications through Off-line Biometric Identification", G. Davida, Y. Frankel, B.J. Matt., *Proceedings of the 1998 IEEE Symposium on Security and Privacy*.
11. National Physical Laboratory, <http://www.npl.co.uk>.
12. "Biometrics: Promising frontiers for emerging identification market", A.K. Jain, L. Hong and S. Pankanti, *Comm. ACM*, pp. 91-98, Feb. 2000.



Since September 11th 2001, innovative technologies have been seen as a way to heighten national security.

By Henning Arendt, Teletrust

Biometric Identification and National Security



Biometric recognition methods would :

- ▶ increase the security of passports and IDs (forgery-proof). Biometric facial and fingerprint recognition could be incorporated into the passport and ID card.
- ▶ unequivocally link people to their identification documents
- ▶ support the personnel controlling access to borders and security zones (airports, airplanes, companies and public authorities)
- ▶ enable automatic recognition of people in hot spots (prevention)

Biometric recognition methods

Biometric recognition methods have been around for a number of years. They are based on the assumption that each person has unique and unchang-

ing characteristics, which can be used for identification with the help of electronic methods. Amongst these characteristics are; fingerprint, face, hand geometry, voice, signature dynamics, iris and retina etc. A distinction is made between static characteristics (finger, face, iris), which only change marginally, and dynamic methods (voice, signature), where the person to be identified has to actively participate/take an action.

Also a distinction is made between passive registration, (e.g. of the face through a camera when walking past) and active registration where the person to be identified has to actively participate (e.g. put the correct finger on the scanner).

Reference data – making a template

Usually the image collected with the first biometric registration is extracted into a smaller “template”. This template is used for reference during the subsequent use. The original image cannot be recovered from the template.

100% recognition – is this possible?

All methods have the same problem in common; that the 100% recognition of a person is impossible. Good approximate values are in a one-digit percentage range. Since each human being regenerates within a few weeks, many of the biometric “unchanging” features are subject to this dynamic change. Furthermore, fashion changes, as well as illnesses



or certain living conditions influence the recognition of once recorded biometric features. Pilot projects in Germany, the EU and other parts of the world have shown that good biometric methods lead to a high recognition rate with most of the test subjects, if the basic conditions are good – high quality enrolment, good user guidance and frequent use which allows the system to adjust the internal reference data to the user.

Problems encountered

In a lot of the comparison groups there are problematic users, who are not recognized at all or only after a great number of tries. Depending on the method used, this problem group can reach a two-digit percentage range – impossible to imagine that out of 80 million German citizens, 10% (that's 8 million) should have problems crossing the border.

Field trials also show that successfully registered subjects are not recognized temporarily.

Stability of biometric methods

Several companies and research facilities are engaged in researching and developing biometric methods. Also, important foreign producers with their German branches and system integrators are involved in projects. User surveys show that the demand for robust procedures usable in everyday life is high.

To accomplish this, projects with a great number of users are necessary (a couple of 1000 users and respectively a good number of biometric terminals) which enable the manufacturers to develop their procedures into professional systems and with a simultaneous recompense of the costs.

Privacy and consumer protection

The privacy commissioner and consumer lawyers are also analyzing biometric identification systems.

Recommendations were developed, (e.g. within the context of BioTrusT) to prevent misuse: among these, the demand that biometric templates should only be used when approved by

the user. A technical solution would be to store the biometric templates on a personal token owned by the user, e.g. a Chip Card. Alternatively other solutions like central storage are possible, if it can be ensured that the biometric template can only be used with the owner's approval. In cases like border controls, a central database will be necessary, otherwise misuse cannot be prevented. Experiences made with cash dispensers have shown that misuse could only be reduced to today's low levels after connecting all cash dispensers to central control centers. Each payment has to be authorized on-line. Which range of applications can be enhanced by biometric identification? Although biometric identification cannot immediately improve national security significantly, it can help to reduce human inefficiency in identifying a person in the medium-term.

► Company ID with a strong tie to the holder

One important use would be to strengthen the link of an employee to a company ID. This is especially important for people with sovereign functions or employed in a high security area, like personnel of airports and airlines.

► Personal identification for electronic systems

Another important area is access to electronic systems. Here misuse can be reduced through the identification of a person. Especially in the area of electronic monetary transactions, the unequivocal identification of a person is to be recommended.

► Support of border controls to ease entry

For frequent travelers, biometric identification could reduce or eliminate border control waiting when entering or leaving a country. A voluntary system – comparable to the American INSPASS or the similar Israeli system – would be preferable to a general mandatory use. Based on these experiences, solutions could be planned nationally. However European cooperation is indispensable,

as most external borders are currently controlled by EU partners.

It has been said that the German passport and ID are among the most "forgery-proof" in the world. Border officials are extensively trained to verify the authenticity of the document and ensure the match of the document to the average German traveler. But it is more difficult to verify the authenticity of foreign documents and to discern unfamiliar faces and features.

The organizational environment however, requires special attention: central or personal storage of the biometric template? Who ensures high quality enrolment? How should problematic groups be managed? How should changes of biometric features be handled and who will carry the cost?

What has to be done?

Before biometric identification can be widely introduced, it is imperative that the systems and procedures are tested with a very large number of real test cases. This test should determine key elements and parameters with enough accuracy to plan for a broad rollout. It should also provide manufacturers with enough experience to develop their methods into products for every day use. Simultaneously it is important to analyze the organizational and financial consequences of a general rollout. A wide social consensus is important; it needs clear and verifiable objectives – what can be achieved with specific costs for implementation and operation of biometric solutions.

[Note: Additionally the question of how witnesses can be protected when strong biometric methods are generally used for national identification must also be considered!]

Many of the experiences described above have been gained from the BioTrusT project. This pilot project was started in 1999 and is still in progress.

"I consider the terrorist attacks on September 11th to be an attack against America's ideals. If our freedoms erode because of those attacks, then the terrorists have won." – Bruce Schneier



BEYOND THE PASSWORD

In today's ever-changing world of information technology, securing critical information and data continues to emerge as the number one concern for all IT managers.

Passwords secure information, but not as securely as IT managers need. Most liken password security to a necessary evil, but few neither believe in the security nor want to manage a password-based security system.

Security Is Just a Fingerprint Away

By Keith O'Leary, Director of Products, Keyware

Keyware is a company that not only recognizes the security benefits of biometrics, but also shares the industry's perception of fingerprint verification as a solid method of identifying an end user. Keyware's biometric strategy is to provide the best-of-breed biometric authentication solutions to IT managers and professionals wanting the strongest possible authentication for their company information and business resources. Keyware provides the platform needed to quickly and effectively roll out strong biometric security measures throughout an enterprise.

According to industry analyst firm, Frost & Sullivan, the market for authentication technologies, including biometrics, will reach \$2.6 billion by 2006. In a response to this ever-growing variety of authentication methods, Keyware (based in Massachusetts, USA and Brussels, Belgium) has created the Centralized Authentication Software (CAS) Server, which allows organizations to manage all their authentication methods (PKI, biometrics, Smart Cards, PINs, passwords, etc.) from one server.

The CAS Server

Keyware's CAS Server (Centralized Authentication Software) enables companies to centrally manage the authentication process on a secure user basis. Providing strong authentication using biometric and non-biometric techniques,

the CAS Server eases the burden for system administrators by establishing a central repository of user authentication policies and methods. Both biometric (finger, face and voice among others) and non-biometric (PKI, tokens and Smart Cards) authentication methods can be combined to manage access to network applications.

The CAS Server helps organizations maximize their biometric authentication investment, allowing them to achieve the perfect balance between security and convenience. Organizations work with the best-of-breed biometric techniques, such as the ID Mouse and ID Mouse Professional from Siemens. Keyware's authentication solutions offer an open and extensible architecture that allows security administrators to leverage their existing infrastructure. The biometric system is centrally controlled and managed by the security administrator, while end users experience fast and even transparent authentication.

Working with Siemens

Siemens' ID Mouse and ID Mouse Professional are the leading fingerprint biometric mice on the market, allowing easy-to-use biometrics for end users in a sleek, fun design. Siemens' ID Mouse and ID Mouse Professional algorithms are fully integrated into Keyware's CAS Server technology. This is an important

What is the alternative? The answer is simple — biometric authentication. Biometric authentication verifies the identity of the user, protecting against the possibility that someone else has gained knowledge of the password. Some would argue that biometric authentication is not simple. I, and many others, believe differently.

Biometrics has come of age and many industry professionals realize the strength of security and ease of management and maintenance biometric security provides. Lost, stolen or shared passwords become a thing of the past, strengthening access to critical resources and easing the burden of continued password maintenance.

According to most of the major high-tech industry analysts, more than 70% of the existing biometric authentication market is driven by fingerprint verification. Fingerprint verification is a proven technology. Fingerprints have been used for decades as an individual identifier by law enforcement and government agencies. It's something that is familiar to all, convenient and most importantly reliable.



step for customers who want to pull together their entire authentication system and manage it from one central location and cut down on the number of peripherals at an end-user's workstation with the dual purpose mouse.

It was important for Keyware to partner with the best of breed fingerprint reader maker, Siemens. ID Mouse and ID Mouse Professional offer Keyware customers:

- ▶ One of the most accurate fingerprint devices on the market – improved algorithm has lowered the False Rejection Rate to the level of 1.3 percent – unprecedented in the industry.
- ▶ Easy enrollment so the end user can initialize the mouse quickly and easily. The end user also enjoys fast authentication.
- ▶ Automatic recognition of tampering and hacking denies access.
- ▶ Security administrators can define several users for one PC.
- ▶ Reference data is stored in a heavily encrypted format (DES3)

For Siemens clients, Keyware's integration with ID Mouse and ID Mouse Professional allows them to:

- ▶ Centrally administer complex enterprise environments, securely managing hundreds or thousands of users and potentially hundreds of authentication policies.
- ▶ Layer different biometric technologies with traditional authentication techniques-layering what you know (PINs, passwords) with what you have (Smart Card, token) with what you are (voice, face, fingerprint) allows organizations to achieve a new level of security.
- ▶ The ability to present confidence levels with the patented "Dynamic Policy Selection." Whenever a user attempts to gain access to a protected application throughout the network, the "Dynamic Policy Selection" will choose the most appropriate authentication policy based on the confidence level assigned to that application and the availability of hardware at the users' desktop.

Providing integrated support for industry-leading third-party applications and technologies, such as Siemens' biometric solutions, is part of Keyware's strategy to deliver out-of-box support for the widest range of biometric security solutions, and enable customers to mix and match best-of-breed products with the CAS Server. Support for Siemens' fingerprint technology allows Keyware customers to seamlessly deploy biometric fingerprint security at any security point within an enterprise while managing it centrally from one server.

With our partnership with Siemens fully in place, Keyware offers a very attractive and complete biometric security solution to many companies in many different industries. A large number of corporations, government agencies, financial institutions, insurance agencies and health care organizations are finding that Keyware and Siemens deliver the IT security they need today and know that the combined solution will scale as their needs grow.

Potential Markets

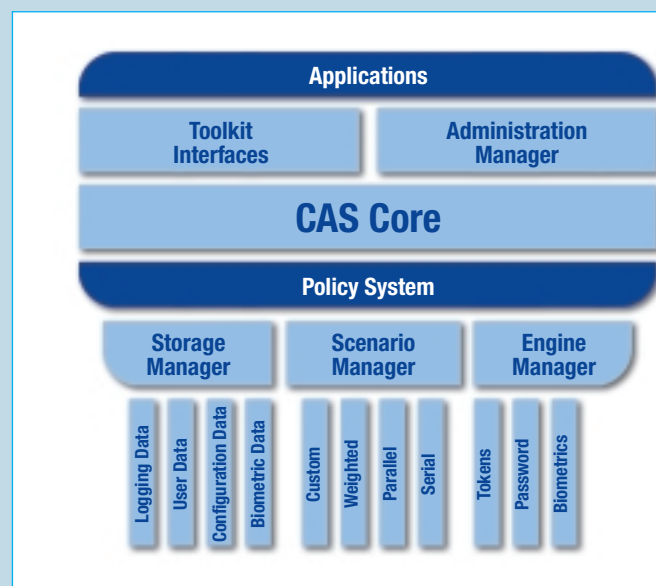
Keyware is talking with a number of banks and investment houses that want stronger security measures without having to sacrifice accessibility and convenience for their clientele. They understand the value Keyware delivers in the CAS solution and they've been seeking a fingerprint device that's both functional, but more importantly, will draw the attention and drive the adoption of the technology with their clientele. When we showed them the Siemens ID- Mouse Professional, the reaction was one of overwhelming acceptance.

The Mouse's attractive design and optical sensing capabilities made it a clear winner. Banks are considering plans to purchase quantities of the mice and programs that will deliver them to their top-tier

clientele for enhanced security through fingerprint authentication.

The Healthcare industry is an extremely active vertical market for enhanced security and Keyware is a dominant player in this segment, deploying strong biometric security products. Privacy of patient data through controlled access is the predominate requirement for most healthcare organizations. Governmental regulations imposed by the HIPAA regulations of 1996, mandate stronger security measures by all healthcare organizations. Biometric authentication ensures that only those authorized gain access to patient information. Fingerprint authentication is what most healthcare organizations are looking for and reaction to Siemens ID Mouse Professional has been exceptional. The fact that the optical sensor works on most any surface has been a big differentiator in the decision process.

More and more industries and enterprises are seeking similar solutions to enhance the security policies and procedures within their organizations as well as outside their organization. Together, Keyware and Siemens deliver the products and solutions that IT managers and IT professionals look for. Bottom line, biometrics is the security function of today and Keyware and Siemens are helping to bring the technology to every desktop.





Infineon's TCPA-compliant security solution supports all PC security applications



By Thomas Rosteck,
Infineon Technologies AG

Communication over the Internet is growing continuously. Many applications, such as those intended for eCommerce, are based on trust in the communication partner and the reliability of the connection. You have to provide authenticity, integrity, and confidentiality/privacy.

With the development of TCPA (Trusted Computing Platform Alliance), a powerful business initiative was launched. Its objective is to increase confidence in the Internet. The TCPA founded by Compaq, Hewlett-Packard, IBM, Intel and Microsoft (now including more than 160 companies), has defined a device – known as the Trusted Platform Module (TPM) – which will assume responsibility for many important security functions. TPM is the root-of-trust in a given platform (e.g. a PC, notebook, and in the future, a mobile phone or PDA). It checks the system integrity – and authenticates third-party users who would like to access the platform – while remaining under complete control of its primary user. Thus, privacy and confidentiality are assured. With TPM-based platforms it will be possible for the first time to create the basis for a worldwide public key infrastructure (PKI). This in turn will ensure the security of many applications for private and corporate environments in particular – while making other types of applications possible for the first time. With an established reputation for cutting-edge and market-tested security technologies, Infineon is the first to market a security solution for all computing platforms. The activities of TCPA and the resulting security standard show the requirements for today's security technology. Infineon's Trusted Platform Module (TPM) architecture is designed to provide both highest security standards, based on proven security technology, and easy system integration by providing a complete solution. The TPM offers the same security features as Infineon's standard security controllers

including non-volatile memory, cryptographic implementations of RSA and Hash Algorithms (SHA-1 and MD-5) for highest possible performance, as well as a true random number generator. One of Infineon's goals is to fulfill the security requirements for all future computing platforms and therefore enables the growth of tomorrow's applications with certified security.

Infineon Technologies TPM offers:

- ▶ 16kByte Non Volatile Memory for the secure storage of keys and secrets
- ▶ HW-RSA-Accelerator (Signature Calculation, Signature Verification and Key Generation@2048bit key – using CRT)
- ▶ Hardware Hash-Accelerator (SHA-1, MD-5)
- ▶ True Random Number Generator (TRNG)
- ▶ The highest possible security levels against SPA and DPA
- ▶ Low power consumption
- ▶ 2 timers and 1 interrupt module
- ▶ LPC interface

Software Architecture:

- ▶ Embedded secure operating system
- ▶ Embedded application
- ▶ Reference implementation for PC-BIOS integration
- ▶ TSS software stack according to TCPA specification
- ▶ TPM Cryptographic service provider (CSP)

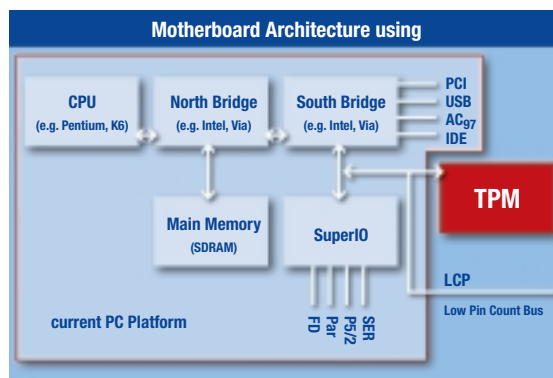
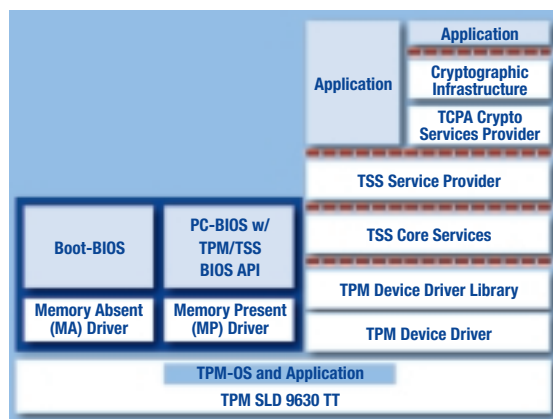
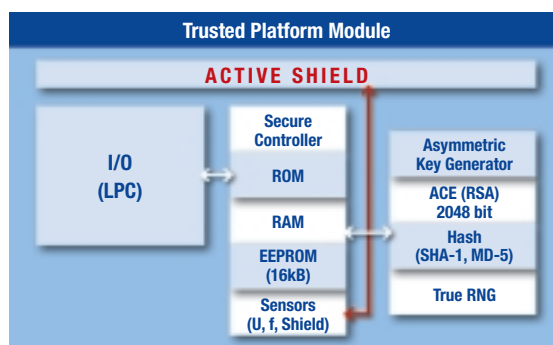
System Integration

To ease integration into virtually every known PC platform, the TPM uses the standardized LPC inter-

face (Low Pincount Interface) as defined by Intel. This has the advantage that a small package can be used.

Furthermore, the bandwidth of this bus is more than sufficient for the intended application (approximately 4Mbyte/s), thus enabling more sophisticated use of an Infineon TPM.

Finally, the necessary support for the LPC is already integrated in every system BIOS since the SuperIO is attached to this bus. This simplifies software integration of the TPM into the BIOS Boot Block.





By OMNIKEY

The CardMan Fingerprint 7120 from OMNIKEY

By combining biometric identification processes with market-proven CardMan Smart Card technology, CardMan Desktop fingerprint does not only improve security conditions – it also allows a much easier handling of Smart Cards in many areas where they have come to be used.

Developed by OMNIKEY, the biometric Smart Card reader stands out against ordinary read/write devices based upon Smart Cards through various innovative product features. From now on, for example, tools like PIN numbers identifying a particular user will not be necessary anymore, a fact which minimizes security risks and improves handling processes. As biometric technology works differently, users can dispense with time-consuming administrative procedures every time access has been denied. Moreover, biometric identification, based upon the unique character of unchangeable fingerprints, benefits from full legal acceptance.

Smart Cards are increasingly being used for applications such as Payments (e.g. Mondex, Visa-Cash, Amex, GeldKarte), Home-Banking, Smart Card based Authentication (Single-SignOn), Digital Signature Internet-Security, e-commerce, PKI-Tokens, Health cards, Loyalty etc. At the same time, biometric technology is needed for a more secure and convenient access to Smart Cards and applications. OMNIKEY's CardMan® fingerprint product-family facilitates the use of Smart Cards in combination with biometrics in PCs, Notebooks, Servers, PDAs and Set-Top-Boxes.

well as health care organizations and public administrations.

The silicon sensor utilizes the biometric fingerprint recognition method. Fingerprints have been successfully used to accurately identify individuals for more than a century. European Courts accept that just matching twelve minutiae is enough for a legal identification. So the technology is well known to users and application providers. Use within an application is

based on standardized interfaces like PC/SC, OCF (Opencard Framework) or CT-API, all in combination with the most important biometric interface – BioAPI. Generally, drivers are available for Windows 98, Windows 2000, Windows XP and Windows ME. CardMan fingerprint is designed as an OEM-product on which customer specific logos, colors or form-factors are possible. The technology is also available as Chip-Set.

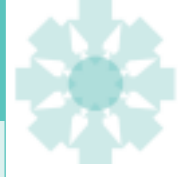


Fingerprint 7120

Biometric identification processes will be used especially for applications that require a high security level, for instance home banking, Internet, access control and computer access, as well as digital signatures. The target groups for CardMan Desktop fingerprint include manufacturers of personal computers, financial and insurance companies as

USB-Smart Card Reader with Fingerprint Sensor

Connection	USB (Universal Serial Bus)
Biometric Sensor	Capacitive Silicon Sensor
Cable Length	180cm
Power Supply	USB
Card Contacting Unit	100,000 insertion cycles
Card Power Supply	60 mA
Status Indicator	Duo-LED
Transmission Speeds	Fingerprint 3 frames/s Smart Card 9,600 – 115,200 Baud
Protocols	T=0, T=1 SLE4418, SLE4428, SLE4432, SLE4442 Others on request
Drivers	PC/SC, Fingerprint –USB
Operating Systems	Windows, 98, 2000 Windows ME, XP Others on request
Certification	PC/SC planned
OEM	OEM-Logo possible, Customer specific colors



Taking care of your business advantages

By Sospita ASA

Ever heard of software reverse engineering? Want to know how you can protect your software from being reverse engineered? Then read on.

Information is Power

In our time where information is power and you have the ability to turn your business focus around in a shorter and shorter time, software has become increasingly more important for solving more complex tasks. Businesses can go bankrupt if their systems are down or their software fails.

This dependence on software has also opened up a whole new market for software developers creating specialized software for specialized markets. When selling software to this demanding market it is, of course a clear advantage to have unique software, or at least software that is better than the competition's.

What sets your software apart from the rest? Most probably it is because you

have developed a new and improved way of software design, or simply have a formula or analysis module that is far more advanced than your competitor's. *And that is where your BUSINESS ADVANTAGE lies.*

Until, someone reverse engineers your software, uncovering your business advantage, and makes it their own. Or even worse, publishes the code on the Internet.

Ever since the early 60's when Dr. Maurice Halstead came up with the notion of the compiler and later the de-compiler, crackers and others have spent their time on de-compiling and reverse engineering software.

The motives of de-compiling or reverse engineering software are of course individual. While some do it for educational purposes, others simply want to exploit software on the market. There are also disgruntled ex-employees whose motive is just plain revenge. In any case, if your source code gets published on the Internet, your business advantage is in jeopardy. Obviously, no one will buy software they can compile themselves.

Let's create a few scenarios to see how reverse engineering can impact a company:

1. The Stockbroker software company

Company X has developed special analysis software for stockbrokers. They have invented a very efficient and smart way of forecasting the trends of specific stocks or bonds. It is one of kind software, and they are making heaps of money, since every financial adviser wants their software.

In their software source code resides the mathematic formulas that are so

groundbreaking and efficient. By reverse engineering their software, a really good cracker (or others) can uncover the ingenious formulas and share company X's knowledge with the whole world.

Suddenly company X's business advantage disappears, and so does their revenue.

2. The Energy Broker software company

Company XYZ is a supplier to the energy broker industry. The energy broker industry needs sophisticated software to be able to sell energy from different suppliers, based on lowest spot prices.

XYZ's software is able to provide faster, better and more accurate models for when to sell and buy, making them the industry leader for this kind of software. Then, someone reverse engineers the software, uncovering the valuable source code.

Suddenly, Company XYZ's business advantage disappears too, and their bottom line is actually the bottom line...

These short case scenarios are just examples of how vulnerable software can be, thus making the company equally vulnerable. There are numerous businesses that rely heavily on their unique software to make their revenue, like financial institutions mentioned in the first scenario. Banking, the health-care industry, insurance companies, etc. are other such industries.

And as in any type of business, you must take good care of your revenue maker.

Naturally you want to keep your source code away from prying eyes. Your software is after all your revenue maker.

Factoid:

Software reverse engineering involves reversing a program's machine code back into the source code that it was written in, using program language statements.

Reverse engineering for the sole purpose of copying or duplicating programs constitutes a copyright violation and is illegal. In most cases, the licensed use of software specifically prohibits reverse engineering.

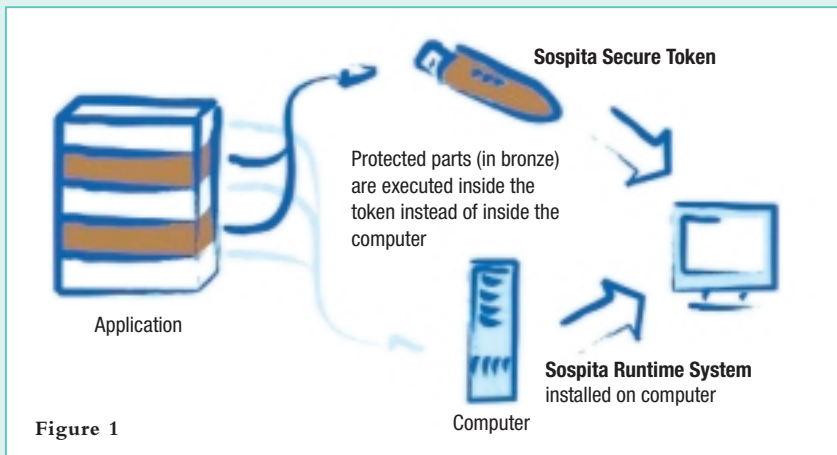
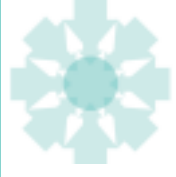


Figure 1

But the hardest part is to protect your source code in a secure, smart and easy manner.

By using Sospita License Protection you can achieve all this.

What is Sospita License Protection?

Sospita License Protection (SLP) prevents unauthorized use of software (piracy or reverse engineering) through a process whereby parts of the protected source code are encrypted. The real high security is obtained through execution of the protected code in a secure, external token, either a Smart Card or a USB token. (Figure 1.)

The focus of SLP is to prevent piracy in a very secure manner, but the principal methods also protect your source code from being reverse engineered. By using the Sospita SDK, you can protect the part(s) of your software that contains your revenue making code. If someone manages to reverse engineer your software they will see your source

code, but the protected parts are not readable.

Sospita can help protect your bottom line.

Reverse engineering scenarios can be avoided by protecting your code with Sospita License Protection.

The SDK is easy to use and integrates elegantly into MS Visual Studio as a plug-in. You don't have to leave your IDE to protect your applications.

When your application is in the final stage of development, you can use Sospita's SDK to mark and encrypt the vital parts of your revenue making source code. (Figure 2.)

The code you protect will be rendered unreadable with 3DES encryption, and the key will be stored in the highly secure Smart Card or USB Token. Before compiling your software your code will appear as garbled text. Definitely not readable! (Figure 3.)

You can see the protected parts displayed in green color. Now you can compile your software as normal, and distribute to your customers and on the Internet, knowing that your business advantage and bottom line are well protected.

Added benefits with Sospita License Protection

While the traditional software distribution model still works, some market segments demand more flexible solutions, like software rental and frequent online updates. For example, the Stockbroker company in the earlier scenario would provide their customer with updated analysis results, and thereby make sure the customers do not have an outdated version installed.

With SLP you can choose from a list of time constraints for your software, and also control what modules your customers can or cannot use. (Figure 4.)

Let's say you're providing Project Management software, you might increase sales if you offer your software for rental.

Most projects have a pre-defined start and end time. Why would your customers buy an unlimited version of software they don't plan to use after 6 months? For these types of customers it would be more cost efficient to rent the software per project. If you establish a good pricing model, both you as a software provider, and the customer, could benefit from software rental. By using Sospita License Protection you can easily do this with the level of security you need.

Figure 2

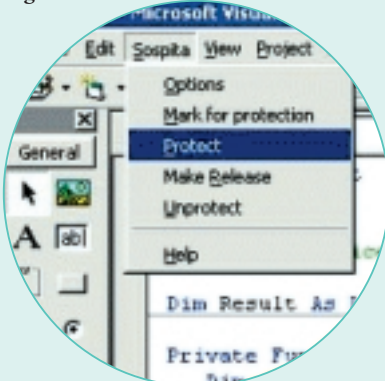
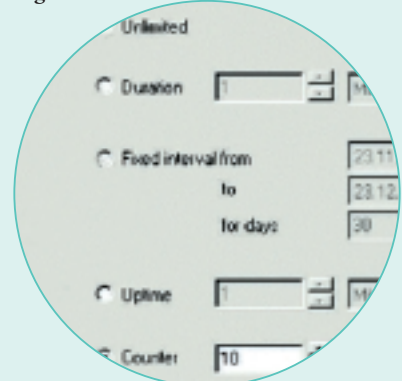
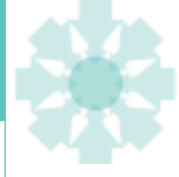


Figure 3



Figure 4





Apollo-CL: The Multi-Application Smart Card OS from SC²

By SC²



The Apollo CL is a natural choice for many applications, including public transport, toll collection or access control as well as for many IT applications, offering easy access to contactless memory through any Type A or Type B reader.

Dual Interfaces, Many Applications

The SLE66CL160S (available from Infineon Technologies AG) contactless interface uses the SC² Apollo CL operating system that is used for a wide variety of Smart Card applications (e.g., e-purse, stored value cards, loyalty, etc.). The Apollo CL has been designed to combine the advantages of both contact and contactless technologies and is the ideal card to extend your current memory and magnetic strip applications, while at the same time leveraging the benefits of contactless technology. The Apollo CL also allows you to extend memory card contactless applications into high-security services. EMV compatibility is also available as an option, upon customer request.

Multi Application Smart Card OS

The Apollo multi-application micro-processor card offers secure payment and data-management features as well as a wide range of applications including:

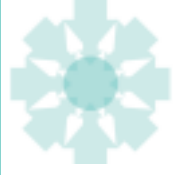
Apollo Product Range

An extended range of E²PROM capacities are also available to cover all customer needs, for both data storage and application implementation.

Product	EEPROM Size (K Bytes)
Apollo CL 7K	1KB – 7KB
Apollo CL 14K	1KB – 14KB
Apollo 32K	32KB
Apollo 64K	64KB

- ▶ **Electronic Purse**
Open or Closed Payment Schemes
- ▶ **Banking**
Debit/Credit, Home Banking, Magnetic Stripe Image
- ▶ **Public Applications**
Identity, Driving License, Health Care, Tolls, Passports
- ▶ **Access Control**
Logical or Physical, Employment Cards
- ▶ **Multi-Purpose**
Car Registration, Loyalty, Retail, Taxi, Transportation etc.

Apollo allows the user to upgrade their applications when necessary, to implement contactless/combi-card technology (using the Apollo CL features), with public key cryptography (RSA/ECC) and with products such as KMS2 (Keys Management System), Personalization, Smart Card Tooling and others from SC².



Features	Description
ISO 7816, 1-3 Compliance	The basic communication protocol is T=1. T=0 and T=14 protocols can be activated optionally in the card upon customer request.
ISO 7816 – 4 Compliance	Commands, data structure (multi-application) and return codes ensuring a wide acceptance of this range by application issuers and terminal manufacturers.
ISO 7816 –5 Compliance	The Customer Registration ID can be implemented.
System Administration Command Set	An enhanced system administrative command set is available for easy card personalization.
ISO 14443	ISO/IEC 14443-3, Type A / Type B, Anticollision & Communication Protocol
E-Purse Features	Electronic purse structure and payment dedicated command set (Debit, credit, balance)
Cryptography	TripleDES, DES RSA (1024 bit), DSA SHA-1, MD5 MAC Proprietary Algorithms, AES Rijndael (Rhine-doll)
I/O Routines	9600 Baud (up to 115,200 Baud)
Dedicated Security Features	PIN management and verification TripleDES algorithm for authentication, secure messaging External Authentication Internal Authentication Hardware Random Generator
Customization Features	Customization features offer the flexibility required to cover all types of applications.

Memory & Security

The Apollo-CL also has a fully accessible EEPROM memory from Contact and Contactless interface (1–14 Kbytes) as well as contactless historic sectors and Memory Access Control depending on security initialization flow.

The card's EEPROM memory is organized into two distinct areas. When accessed by the contact interface, the memory management relies upon ISO/IEC 7816-4 file structure and commands.

File access can be secured by secret code presentation and/or external/internal authentications using diversified session keys and signatures, both calculated using the triple DES cryptographic algorithm.

In contactless mode, the memory is divided into 16 or 8-byte blocks. These can be used as generic data blocks or value blocks with an optional built-in backup mechanism. Block access is controlled by mutual authentication using sets of secret keys associated with groups of 1 or 15 blocks.

This structure lets you use the same card for different applications without sharing any sensitive information (e.g. cryptographic keys).

Command Set and Data Organization

The Contact Interface works according to ISO/IEC 7816 and the Contactless Interface according to ISO/IEC 14443. Shared memory data access via the contact interface is implemented by creating special files, ensuring security from both sides. You can also limit operations to decrement and read commands from the contact or contactless interface, thereby blocking credit operations over the contactless interface.

Capacity	From 1 to 14 Kbytes contact EEPROM shared from contact and contactless interface
Number of reads	Unlimited
Number of writes	More than 500,000
Data Retention	10 years

Running Commentary

Talk about biometrics rolls on. Only the other day the European Commission convened a forum for biometrics folk to get together in Brussels and hold open discussions about the means of accelerating biometric adoption. Many threads of discussion were followed, from the political to the technical; and from where I sat much time was spent in discussion about the need for a better understanding of business models and for a greater level of trust in local or client platforms. Seen from the crow's nest, there was also interesting discussion as to whether efforts should be focused on pushing biometrics, or in stimulating the pull, clarifying the added value of biometrics as such arguments are unavailable a priori.

As with this issue of SECURE, the typical lack of trust in client technologies was identified as a barrier to adoption. Discussion in these pages shows how many focused efforts are underway to address this push issue. Encouragingly these also support much of the European political agenda about privacy and user ownership of credentials; but that, as they say, is perhaps not important right now.

On the pull side, an identified inhibitor was the fear amongst the potentially large users of biometrics that deployment of complicated user credentials in large networks could go completely out of control, both in their total cost and their security management, which means yet more cost through patched fraud solutions. Large users are still riding the roller-coaster curve, digesting the potential advantages of moving over to PKI certificate-based authentication systems. One conclusion, a majority opinion on the day, was that biometrics might only follow PKI. Few however, were willing to say how closely, but felt that extensive use of PKI would need to be established first for confidence in the management of biometrics to follow. This seems dangerous to me, and for biometric technologies, unfortunate too.

I'd like to hazard more than a guess that PKI is going nowhere interesting without biometrics and secure local platforms for credentials management. If it then goes nowhere by itself, then there is a likely risk that nothing will follow, based on a misplaced belief that we

cannot build on failed technology. Fundamentally, the argument for PKI is complex; it offers complicated cost calculations to those considering implementation, mainly to do with the ramifications of implementing a public key certificate structure. Private key issues are therefore often looked on as trivial and secondary, and unworthy of preparatory effort.

What is the most interesting thing about PKI? For me, it has to be as the enabler of two parties to remotely trust each other in four different ways across the no-man's land of electronic business. The four-fold package offers: Privacy, Authentication, Integrity, and Non-Repudiation (or P-A-I-N for those who implement badly). What would inadequate key security entail? Certainly a weakening of this value package; where would the privacy of information be if the identity of the encryptor/sender were in doubt? The value of authentication via PKI is potentially wiped out if the host system cannot be reassured that the private key is in the right hands. Message integrity, like confidentiality, is only preserving and transmitting the original identity of the source of a message. Finally, what does all the emerging global e-signature legislation mean in practice when non-repudiation can be undermined by demonstrations of poor private key management or even the exceptional evidence of this? The burden will be strongly on the shoulders of the service wishing to benefit from non-repudiation

that it provides a robust key management audit if it wishes later to litigate on its claims. Too much emphasis has been given over to secure transport value in PKI, and not to one of the fundamental objects of this, the identities of the parties.

Instinctively, at the last minute, service providers lurch towards central PIN control of keys: protocols are formed, helpdesks are set up, new password replacement routines are implemented, and mother's maiden names are gathered by the thousand, penned into new databases of users' information. Paradoxically, while these costs are being incurred, the system is working backwards; first designed to implement trust on a distributed and anonymous basis, the distribution of PIN secured keys creates a second, long-lasting management problem that can only be confidently solved through the centralized interrogation of users. In the worst case, costly certificate revocation will grow as fast as password refreshment if confidence in the key integrity is undermined. This may even put dangerous economic pressure on passwords to stay unchanged even when they might be compromised.

If we can point confidently to local security of key management then we can go a long way to the stable quantification of the distributed costs of PKI, and will perhaps see increasingly earlier adoption of such systems with biometrics as a staple ingredient.

