Security on the Move

At the Border for Biometric Passports
Trusted Transaction Roaming
Smart Proof of Citizenship
The mobile world is finally upon us. With a saturation of mobile phone users worldwide there is a renewed emphasis upon phone manufacturers, operators and service providers to enhance and upgrade their range of services and applications. In other words, we are on the edge of the changeover from voice to data oriented services that are accessible from your mobile phone.

This in itself brings a whole new set of challenges for the market in terms of security and co-operation for a suitable, safe, trusted environment for these services to work and be widely accepted. The Radicchio Association has made some progress in this arena, with their trusted transaction roaming (t2r) proposal that appears to be making headway with a number of global players within the mobile industry. You can read more about this on page 12.

Once again, proposals of a widely incorporated biometrics identification project have appeared on the scene. The difference between these projects and others that have appeared in the past is the new interest of governmental agencies. In this issue of SECURE, we are talking about the use of biometric identification technology being incorporated into passports. After all, a passport is the closest thing that anyone has to an officially recognized form of identification. If biometric identification technology is to achieve a mass acceptance status – then this could be the application that enables it on a global scale. Setec's article on page 21, explains more about this particular subject, as well as SC²'s article on the triumphs and tribulations of issuing an identification card in Israel on page 26.

As usual, this issue of SECURE is packed with all the latest news from the Silicon Trust partners, as well as the latest information on a whole range of security technologies from WLANs to smart cards.

Who knows - a few years from now, you may be reading SECURE via your phone!

Dr. Jürgen Kuttruff  
Head of Security Group  
Infineon Technologies
Highlights

6 What's new at Infineon Technologies

The Silicon Trust

8 Introducing the Silicon Trust
9 Welcome to the Trust

Industry Initiatives

10 The Smart Card Centre at Royal Holloway University of London
11 The Institution of Electrical Engineers

Application Focus
Secure Mobility

12 Trusted Transaction Roaming
By Stefan Engel-Flechsig, Radicchio Ltd.

18 Who's Listening on your WLAN?
By Dr. Peter Laackmann, Infineon Technologies AG

Application Focus
Identification

21 At the Border for Biometric Passports
By Pekka Kariola, Setec Oy

24 Smart ID for the man on the street
By Olivier Chavrier, Gemplus

26 Smart Proof of Citizenship
By SC²

28 The Card that Cares
By Michael Nitz, Giesecke & Devrient

Technology Update
Smart Cards

32 Integral Security from FLASH to ROM
By Dr. Peter Laackmann, Marcus Janke, Infineon Technologies AG

36 Single Event Effects – Security Controllers under Attack
By Dr. Peter Laackmann, Marcus Janke, Infineon Technologies AG

Within the Trust

40 BIOPASSPORT® Enterprise Server
By IdentAlink

42 Multos Products for Migration and Security
By Keycorp

43 Explaining the SyntiQ Solution
By SyntiQ

44 realtime Security in Brevard County
By realtime

46 Wave Systems’ EMBASSY® Trust Suite Portfolio Enables Secure Business Computing
By Wave

48 Running Commentary
By Mark Lockie

50 SECURE Subscription Form
How to Contact this Issue’s Authors

Industry Initiatives

Page 10
Dr. Keith Mayes
Director of the Smart Card Centre
Tel: + 44 1784 414408
keith.mayes@rhul.ac.uk
www.isg.rhul.ac.uk

Page 11
Paul Mathews
Professional Network Manager
The IEE
Tel: + 44 1438 765635
pmathews@iee.org.uk
www.iee.org.uk

Application Focus – Secure Mobility

Page 12
Stefan Engel-Flechsig
Radicchio Ltd.
Tel: +49 172 944 70 93
stefan.engel-flechsig@radicchio.org
www.radicchio.org

Page 18
Peter Laackmann
Infineon Technologies AG
peter.laackmann@infineon.com
www.infineon.com/security

Application Focus – Identification

Page 21
Setec Oy
Tel: +358 9 89 411
info@setec.com
www.setec.com

Page 24
Carl Norell
Gemplus
Tel: +1 215 390 2899
Carl.NORELL@gemplus.com
www.gemplus.com

Page 26
Jacob Mendel
SC² Ltd
Tel: +972 3 765 7 369
jacob_me@netvision.net.il
www.scsquare.com

Page 28
Michael Nitz
Giesecke & Devrient GmbH
Tel: +49 89 4119 2640
michael.nitz@de.gi-de.com
www.gi-de.com

Technology Updates – Smart Cards

Page 32 + 36
Peter Laackmann, Marcus Janke
Infineon Technologies AG
peter.laackmann@infineon.com
marcus.janke@infineon.com
www.infineon.com/security

Within the Trust

Page 40
Elmar Hilgers
IdentAlink
Tel: +49 30 63926970
ehilgers@identalink.com
www.identalink.com

Page 42
Graeme Bradford
Keycorp Limited
Tel: +61 2 9414 5303
grbradford@keycorp.net
www.keycorp.net

Page 43
Jolanda Zuijdendorp
SyntiQ International BV
Tel:+31 162582175
jolanda.zuijdendorp@syntiq.com
www.syntiq.com

Page 44
Thomas Neudenberger
realtime North America Inc.
Tel: +1 813 283 0670 ext. 703
thomas@realtimenorthamerica.com
www.realtimenorthamerica.com

Page 46
Brian Berger
Wave Systems
Tel: +1 949 716 3116
bberger@wavesys.com
www.wave.com

Running Commentary

Page 48
Mark Lockie
Ideal Media Consulting
m.lockie@btopenworld.com
At the beginning of June, the 5th Security Solutions Forum took place at the Marriott Hotel, Munich. The biannual Solutions Forum consists of two parts: Day 1 is dedicated to the Silicon Trust Partners, whereas Day 2 takes the form of a Security Conference and is by invitation only.

Day 1 began with a strategic overview of the Secure Mobile Solutions Group, stressing the inevitability of the need for security in a more and more mobile world. The Silicon Trust Partners present had the chance to discuss with Infineon Management, amongst other topics, the changes that are taking place in the security value chain.

For the remainder of the day, Partners were able to catch up with Infineon Technologies SMS Product Roadmaps and Strategy Updates, as well as mingle in the Mini-Exhibition that was set up in a nearby room.

Day 2 was a huge success: nearly 100 participants accepted the Silicon Trust invitation to listen to the tightly packed presentation schedule. The agenda was split into 3 sessions:
- Secure Identification
- Wireless Security
- Secure Computing.

Each Session consisted of three Business Case Presentations, with Speakers from Silicon Trust Partners, Infineon and guest companies. The most enthusiastic attendee feedback was received for the Infineon presentation on the necessity of WLAN Security, where the presenters using simple equipment and software downloaded off the internet, showed everyone in the room just how easy it is to locate and interpret data from a WLAN Access Point.

Infineon Helps Bring New Level of Security to Computer Networks

Infineon Provides Embedded Security Chip Solution for New HP Compaq Business Desktop PC

Infineon Technologies has announced that it now provides the standards-based Embedded Security solution for HP’s d530 series business desktop PC. The new HP ProtectTools Embedded Security chip enhances the security features of the desktop’s native operating system and third-party security applications, bringing a new level of data protection and access control to networked computers.

Infineon worked closely with HP to integrate a Trusted Platform Module (TPM) compliant with specifications published by the Trusted Computing Group (www.trustedcomputinggroup.org). Infineon also collaborated with HP to develop the system’s user-friendly Security Management Software application and the HP Personal Secured Drive, which simplifies data protection through file and folder encryption protected with hardware-based key generation and storage.

“We are very proud to extend our long-term relationship as a key supplier of components for HP Compaq systems and help the company be one of the first providers of this important new security technology,” said Ulrich Hamann, former Chief Executive Officer, Secure Mobile Solutions Business Group, Infineon Technologies. “This program also represents one of the first publicly announced examples of Infineon’s success in delivering a complete solution in collaboration with a systems customer, marking an important milestone in the company’s Agenda 5 to 1 strategy.”

“The Embedded Security option for the d530 series helps HP give businesses the tools to protect valuable data, without sacrificing the performance, reliability and excellent lifecycle ownership costs that are the hallmark of HP systems,” said Brian Schmitz, Worldwide Senior Product Marketing Manager, HP Business Desktops. “Infineon provided outstanding support to our product teams in turning this important and complex technology into a world-class, seamlessly integrated solution.”

Infineon was one of the first semiconductor companies to release a complete Trusted Platform Module compliant with the Trusted Computing Group (TCG) Main Specification 1.1b. TCG specifications define hardware/software solutions to support a hardware-based public key infrastructure (PKI) implemented in any computing device that interacts with other systems and networks.

From September 1st, 2003, Dr. Erk Thorsten Heyen took over worldwide responsibility for Infineon’s Secure Mobile Solutions (SMS) group. The physics graduate began his career in 1992 at McKinsey & Company as a member of the Telecommunication Practice. Between 1996 and 2001 he performed various management functions in different business areas at Bertelsmann AG, primarily in the sector of electronic media. His last post there was Chief Financial Officer of the E-Commerce Division. From 2001 to 2003 Heyen was CEO at Unit.Net AG.
Highlights

Infineon Technologies and the German Federal Ministry of the Interior Form Security Co-operation

On the 30th June, 2003, the German Federal Ministry of the Interior (Bundesministerium des Inneren, BMI) and Infineon Technologies announced that in the future, they will be closely co-operating in the field of IT Security. BMI Minister Otto Schily and Dr. Ulrich Schumacher, President and CEO of Infineon Technologies AG, have signed a “Memorandum of Understanding” to initiate this security co-operation.

The far-ranging security co-operation between BMI and Infineon aims to establish a sound technology basis for an enhanced security level in Information Technology (IT) systems that are used in the Civil Service, private companies and households. The contracting parties have agreed upon a close information exchange in three subjects: the security aspect in the field of smart card technology; security of future mobile applications; and the security components needed to elevate the trustworthiness of personal computers and computer networks. Furthermore, BMI and Infineon intend to drive selected projects, as a way of promoting the use of secure information technologies in Germany. An example of such a project would be the German citizen card incorporating a digital signature or “Bund-Online 2005”; a government initiative to make all designated Civil Service information services available online to German citizens by the year 2005.

The discussions covering smart card security center on the technological considerations that form the basis of new electronic identification cards and an omnibus concept for a qualified signature card. This signature card planned for every German citizen, would incorporate biometric functionality and be utilized for a wide range of applications, such as Civil Service, job and health related functions.

The topic of security for personal computers and PC networks includes the security standards set out by the “Trusted Computing Group” (TCG). The TCG is an industry initiative that aims to standardize the requirements for a trustworthy PC and to secure it against virus attacks and unauthorized manipulation.

When reviewing the topic of secure mobile solutions, the BMI and Infineon expressed their aim to jointly develop both application scenarios and a trustworthy mobile platform. The results of the cooperation would enable cellular phones and other mobile devices to encrypt data and authorize payments.

“Our information society gets more and more mobile and is in need of new security mechanisms. Reliable communication and information technologies are necessary to secure our computer systems and networks against unauthorized use and manipulation,” said Minister Otto Schily.

“The intensive co-operation with Infineon will enable the speedy availability of security for our citizens. It will also help to modernize Civil Services and to offer new services that are more citizen-friendly.”

“Advanced silicon-based technologies enable a broad spectrum of flexible security solutions for future ID documents, mobile communication devices, PCs and networks,” said Dr. Ulrich Schumacher, President and CEO of Infineon Technologies AG. “Security co-operation between government and the private sector – such as the one between the German Federal Ministry of the Interior and Infineon – and the subsequent use of silicon-based solutions, have the potential to make Germany the pacesetter for such security solutions in Europe.”

Dr. Ulrich Schumacher, President and CEO of Infineon Technologies AG and BMI Minister Otto Schily.
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.

What is the Silicon Trust?

The Silicon Trust Program has, over the last few years, become a well-respected and established Partnership Program within the Security Industry, and has certainly achieved its initial goal of raising awareness for Silicon-Based Security.

As one of the first such Partner Programs in the market, Infineon has demonstrated that bringing together a network of Security Partners can improve the relationship with the end customer, by offering a complete solution across the Value Chain. Building on its past success, Infineon now believes that the Partnership should be widened to include more products and solutions - to provide the Customer with more choice.

And Infineon means to do this by focusing internal resource on continuing to build up solid relationships with companies working with Infineon products, as well as fostering new relationships with companies who are attempting to bring about changes for the future of the security industry – working together to increase marketing and promotional offerings in the marketplace.

What are the benefits of being a Partner?

Working together with Infineon and other companies in the same Market, will lead to a better understanding of applications and future market trends and ensure more influence on Infineon’s direction when developing tenders or discussing future product specs.

Companies can work together to research and formulate Business Cases within an environment of trust and develop integrated solutions for a combined customer base. And promoting the Program as a whole, individual companies can benefit from the resources applied by Infineon.

What are some of the planned activities?

Silicon Trust activities will be a mix between Marketing and Promotional, and the more time and resources invested by the Partner to participate, the better the result. Below are just some of the activities currently being planned for the Silicon Trust:

Activities for the Partners
- Access to a database of Partner contacts
- Behind the Scenes tours of Fab facilities
- Business Case Research & Development
- Participation with Infineon at Exhibitions & Shows
- Web Portal: www.silicon-trust.com
- Secure Application Reviews; in-depth whitepapers about specific market segments
- Secure Magazine
- Security Solutions Forums
- Annual Security Solutions Buyer’s Guide

Members of the Silicon Trust

- ACG
- Aladdin
- Association for Biometrics
- Aspects Software
- Austria Card
- Baltech
- beyondLSI
- Card etc.
- Cherry
- Gemplus
- G&D
- G&D
- Guardednic Solutions
- IdentAlink
- IEE
- Ikendi
- ISL
- Keycorp
- MMCA
- Novacard
- Omnikey
- Precise Biometrics
- PSE
- realtime
- SC2
- SCM
- Secartis
- Setec
- Siemens ICM
- Smart Card Centre
- SyntiQ
- Teletrust
- Tresor
- United Access
- Utimaco Safeware
- Wave Systems

For more information visit: www.silicon-trust.com
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.

**Aspects Software**  Aspects Software is a leading independent provider of operating systems, test and development tools for smart cards.  [www.aspectsoftware.com](http://www.aspectsoftware.com)

**Austria Card**  As a subsidiary of the Central Bank of Austria (OeNB), Austria Card is the competence center for the development and production of smart cards in Austria. [www.austriacard.at](http://www.austriacard.at)

**card.etc**  card.etc AG is a full service provider for integrated smart card solutions and issues multifunctional smart cards for public transport. [www.cardetc.de](http://www.cardetc.de)

**Cherry**  Cherry's products include security keyboards with integrated card readers, keyboards with integrated fingerprint sensors, and smart card readers for many different security applications. [www.cherry.de](http://www.cherry.de)

**Gemplus**  Gemplus helps its clients offer portable, personalized solutions in areas including mobile data services, banking, identity, WLAN, m-commerce and many others. [www.gemplus.com](http://www.gemplus.com)

**IdentAlink**  IdentAlink's security software cuts network administration costs by replacing passwords with biometrics and technologies like smart card, PINs, or passwords. [www.identalink.com](http://www.identalink.com)

**IEE**  The IEE is the largest Europe-based body for professional engineers, with members ranging from students to leading figures in industry, R&D, consultancy, and education. [www.iee.org.uk](http://www.iee.org.uk)

**Keycorp**  Keycorp is a global provider of secure electronic transaction solutions, from cards and terminals to network carriage and payment engines. [www.keycorp.net](http://www.keycorp.net)

**realtime**  realtime offers bioLock, the first SAP-certified fingerprint access and function control for SAP.  [www.realtimenorthamerica.com](http://www.realtimenorthamerica.com)

**Setec**  Setec develops and manufactures high-security smart cards and visual ID products for reliable identification of people over networks and in face-to-face environments. [www.setec.com](http://www.setec.com)

**Smart Card Centre**  The ISG Smart Card Centre researches, develops and provides training on smart cards and related technologies. [www.scc.rhul.ac.uk](http://www.scc.rhul.ac.uk)

**SyntiQ**  SyntiQ creates solutions to reduce cost-of-ownership and accelerate time-to-market of new functionality for remotely controlled devices for payment terminals and ATMs. [www.syntiq.com](http://www.syntiq.com)

**Tresor**  Tresor focuses on mobile security and has developed a mobile phone that utilizes military-level encryption for voice and data transactions. [www.tresor.co.uk](http://www.tresor.co.uk)

**United Access**  United Access is a security provider who makes solutions work as support partner for the Infineon smart card OS SICRYPT.  [www.united-access.com](http://www.united-access.com)

**Utimaco**  Utimaco Safeware AG provides professional software solutions for device and transaction security, e-mail security, digital signatures and PKIs.  [www.utimaco.com](http://www.utimaco.com)

**Wave Systems**  Wave Systems Corp. is an industry leader in developing trusted computing platforms and services to enable secure platform services, infrastructure and e-commerce services.  [www.wave.com](http://www.wave.com)
The Smart Card Centre at Royal Holloway University of London

By Dr. Keith Mayes, Dr. Kostas Markantonakis, Smart Card Centre

The Smart Card Centre at the Royal Holloway University of London was created to provide a worldwide centre of excellence for training and research in the field of smart cards, tokens, applications and related technologies and is situated within the prestigious Founders building.

The Centre, which is part of the world renowned Information Security Group (ISG) was founded in October 2002 by the Royal Holloway University of London, with support and funding from Vodafone and Giesecke & Devrient.

The Information Security Group (ISG) has a well-established MSc program that is training new experts for the information security industry. Each year around 200 students, complete their MSc in either Information security or Secure E-Commerce.

With the MSc program generating growing interest in both the practical aspects and implementation of security solutions, the Smart Card Centre was an ideal complement to the existing work of the ISG.

In the first few months of the Centre’s existence, more than 15 MSc students signed up to smart card related projects and a PhD program has recently started. Work is also at an advanced stage to introduce a smart card course-module as part of the MSc syllabus, so that students may qualify with a specialty in cards/tokens. There are also discussions to establish intensive courses for SMEs, (Small/Medium Enterprises) which would have a stronger business and practical focus to help identify and grasp new opportunities in the smart card area.

It is a goal of the Centre to expand its research activities by encouraging further industry participation. There is a funding aspect to this, but equally, a wish to benefit from the expertise of the partners and ensure that results from the Centre are seen as balanced, cross-company views. The Smart Card Centre’s industrial partners will not only benefit from public recognition of their contributions to research, early access to new developments and the chance to find new expert employees, but also from a range of networking and marketing opportunities.

Work is on-going to allow additional companies to become formal members of the Centre, but in the meantime there is great support from the Founders as well as a number of other valued supporters. For example;

- Giesecke & Devrient has supplied a range of advanced SIM card development tools, supporting SIM Toolkit, Java and browser approaches
- Infineon is supporting an MSc project by making available some low-level development tools
- Mondex (Mastercard) has donated a range of computer equipment, tools and cards for general project work
- Gemplus is installing some sophisticated equipment for side channel attacks
- ORGA has delivered SIM Toolkit development tools
- Barnes International has provided an EMV profile test tool

Supporters have also been providing lectures to support our expert seminar program. The list already includes Vodafone, G&D, Gemplus, Swisscom/SICAP and Mondex.

Not surprisingly, the Centre is attracting a growing number of visitors and a common question is - “What is new in the world of cards, tokens, biometrics etc?” In response, it is planned that the Founders lab will gradually become a “show-case” area for professional demonstrations – with student work moving into a larger space. This has increased the current interest in acquiring a range of demonstration and evaluation kits, including contactless card, biometric plus card, application management and access control systems. This represents a low cost/effort opportunity for industrial supporters to have their products seen by a wide range of visitors.

The Smart Card Centre is privileged to be associated with the Silicon Trust and there is close synergy with partners that are implementing practical but Hi-Tech security products.

The next 12 months will be an exciting time for the Smart Card Centre and also an opportunity to further strengthen links and co-operation with the Silicon Trust.

For more information visit: www.isg.rhul.ac.uk
The IEE

The IEE (Institution of Electrical Engineers) is the largest Europe-based body for professional engineers – almost 130,000 of them. Ranging from students at the start of their careers, to leading figures in industry, research and development, consultancy and education; all of who are working in power engineering, communications, electronics, computing, software, control, informatics and manufacturing. Around 30,000 of these engineers are based outside of the UK.

The IEE, as a professional body, accredits degree courses and post-graduate industrial training schemes, as well as organizing a range of best-practice events – from lectures to major conferences. The body also publishes technical magazines, including on-line titles, as well as specialist books. In addition to these events and its publishing activities, the IEE also operates the world’s leading electronics and physics database – INSPEC (as well as other information services).

What’s more, the IEE also promotes Professional Development including the running of a providers database and has close links with industry through its notable Business Partners scheme.

The IEE’s 36 Professional Networks are world-wide groups of people with common technical or professional needs and interests. Each network provides a home, or focal point, for a community of engineers, and enables them to network, share knowledge and keep up to date with developments in their particular industry or profession. These professional networks are supported by an interactive community-relevant website.

Embracing Change

The IEE has a distinguished history of embracing change – it was started in 1871 by a group of telegraph engineers (sometimes referred to as the Victorian Internet) – and went on to include electrical engineering, electronics and manufacturing. This ability to reflect the changing face of technology is clearly demonstrated by the range of Professional Networks:

- Aerospace
- Antennas and Propagation
- Automotive and Road Transport Systems
- Buildings Electrical Technology
- Communication Networks and Services
- Concepts for Automation and Control Consultants
- Control and Automation Systems Technologies
- e-Infrastructure: Networked Software and Systems
- Electromagnetics
- Electromagnetic Compatibility (EMC)
- Embedded and Real-Time Systems
- Engineering for a Sustainable Future
- Functional Safety
- Healthcare Technologies
- History of Technology
- Human Factors Engineering
- Management
- Manufacturing Enterprise
- Materials and Devices
- Measurement, Sensors, Instrumentation and NDT
- Mechatronics and Robotics
- Microsystems and Nanotechnology
- Multimedia
- Communications
- Photonics
- Power Conversion and Applications
- Power System Equipment
- Power Trading and Control
- Radar, Sonar and Navigation
- Railway
- RF and Microwave Engineering
- Satellite Systems & Applications
- Signal Processing
- System on Chip
- Systems Engineering
- Visual Information Engineering

As a technical authority, the IEE is responsible for the Wiring Regulations (the British Standard to which the industry works), as well as playing a major part in many other areas of national and international standards through such bodies as CENELEC and IEC. It acts as the voice of the profession and sets standards of conduct for that profession.

A major role that the IEE undertakes is in promoting public awareness of how important engineering is in today’s society. A vital contribution is its educational activities service aimed at supporting teachers of science and technology. It has created a portfolio of support including the Faraday Lecture which attracts an audience of some three million people.

The IEE has a network of local Branches including special Younger Members’ sections operating throughout the UK, as well as members from China and Hong Kong, Australasia, Southern Africa, Europe and North America. The body also has outstanding conference centers in London, Birmingham and Glasgow.

The work of the IEE at a glance:

- Represents the profession of electrical, electronic, manufacturing and systems engineering and related sciences.
- Acts as the voice of the profession in matters of public concern and assists Government to make the public aware of technological issues.
- Sets standards of qualifications for professional electrical, electronics, software, systems and manufacturing engineers.
- Accredits degree courses in subjects relevant to electrical, electronic, manufacturing and information engineering at universities and colleges around the world.
- Accredits professional development schemes for engineering graduates.
- Awards scholarships, grants and prizes.

For more information visit:

www.iee.org.uk
Soon, there will be one billion cellular phone users worldwide. Half of these will be using their mobile terminals to access the wireless Internet daily. Mobile communications devices, in whatever form, offer ideal characteristics for undertaking electronic transactions, regardless of location. Since personal communications devices contain the capability for transactions based on tamper-resistant hardware, they will enable a huge (and growing) percentage of the world’s population to participate in secure e-commerce. The combination of e-commerce services with the inherent advantages of the mobile device, will benefit businesses and consumers alike. Major market players are already in the process of establishing trusted infrastructures that will make secure, high-value transactions from mobile devices across wireless networks a part of everyday life.
Secure Mobility

Challenges faced by Mobile Network Operators

Mobile Network Operators (MNOs) used to offer their subscribers just one type of service; voice. Slowly, data services made their way into the portfolio, as can be seen in the case of the Short Message Service (SMS), which became a pioneer in its field and a huge success worldwide. Nevertheless, the emerging data features also had a downside: enabling subscribers to access the Internet suddenly meant that other businesses could easily reach the MNO’s subscribers through their websites. As was the case with ISPs, MNOs feared being relegated to the role of “pipes” between their subscribers and new service providers. These concerns caused them to take protective action. Many MNOs blocked their subscribers from accessing sites that did not offer the MNO direct business value in terms of revenues. However, several countries’ Telecom Regulator Authorities took action and urged operators not to implement such protective measures, in order to let end users benefit from a wider variety of services and a healthier price structure.

The actions of the regulators put Mobile Network Operators back in the awkward situation of not knowing exactly how to leverage their subscriber relationships. Merely offering voice and limited data services (SMS) was no longer a distinguishing factor, since these had become commodity services and were subject to fierce price competition. New competencies and skills were required to offer attractive content and applications to consumers. The MNOs could be considered as still in their learning phase and trying to find new business models based on unmet needs in a changing wireless eco-system.

At the same time, new alternative technologies have emerged on the market to enable wireless connectivity and Internet access: Wireless Local Area Networks (WLANs) connect various handheld devices to a local base station, which in turn is connected to the Internet through a regular landline. The most popular method is the “802.11b” standard, which has already been widely adopted in the United States. Using a compatible handheld device and the 802.11b local area network, the user can, for instance, surf the Net at rapid speeds (up to 11Mb/s) and access a variety of services without any need for a Mobile Network Operator’s conventional network (GSM/TDMA or CDMA).

In parallel with these developments, Mobile Network Operators have invested heavily in the next generation of wireless networks (3G), which provide higher bandwidth (up to 2Mb/s) and will supposedly enable more compelling content and applications. These wireless networks are designed to be able to deliver mobile multimedia, music and video downloads to handheld devices. However, some analysts question the value of this higher bandwidth on the move, especially when Local Area Networks (LANS), such as 802.11b, offer much higher data throughput speeds.

MNOs have found themselves in a position where they have to justify why it is worth accessing the Internet through their networks and not by other means (such as 802.11b LANS). The smart cards that already exist in their infrastructure can help them do this. Figure 1 illustrates the different options that consumers have for accessing data content.

Security in today’s 802.11b networks could also be considered poor. The standard does not include a real security mechanism, which makes it relatively easy for a third party to eavesdrop on the traffic in the networks. Therefore, it can be argued, using an 802.11b network for accessing the Internet and conducting e-commerce is a scenario that may not currently offer sufficient security or trust.

![Figure 1: Options for accessing data services](image-url)
In contrast to 802.11b, a stable security mechanism was built into the GSM standard from day one, in order to enable secure network access. This was achieved by relying on SIMs (Subscriber Identity Modules), which is a type of smart card.

**Challenges faced by Service Providers**

Service providers, both wired and wireless, are looking for better relationships with their customers. When a bank sets up its Internet site using the HTML protocol, it has to go through its Internet Access Provider at some point. Nevertheless, this would be a proprietary solution for a limited market and would require new hardware and software for it to take off.

When a Service Provider chooses to make its online services available wirelessly, it faces many questions:

- Which device will be most convenient for the end user?
- What security level do we want to offer our customers?
- Which network and coding protocol do we intend to implement? (GSM/CDMA/802.11b? or HTML/WAP/I-Mode?)

In terms of security, GSM definitely has the advantage, since its architecture offers secure, “tamper-proof” storage. This feature is due to the removable SIM smart card embedded in the GSM device that enables the subscriber to access the network securely. The same smart card could also be used for a variety of other purposes, such as secure mobile banking, identification, and privacy management. Nevertheless, in today’s world, the SIM is the property of the MNO. This means that nothing can be done with it without first consulting the MNO.

In order to utilize the smart cards’ capabilities in the GSM devices, many banks have teamed up with Mobile Network Operators to offer secure wireless financial services based on the SIM. Other banks have relied on a lower level of security and have simply set up their own WAP or I-mode site for financial transactions without using the SIM or the experience and help of the Mobile Network Operators.

Those who have relied on the SIM and its capabilities, have a very secure solution in place, but have also experienced issues relating to the MNO’s ownership of the SIM. Having cryptographic keys that enable secure access and identification in place, but have also experienced issues relating to the MNO’s ownership of the SIM. Having cryptographic keys that enable secure access and identification in place, but have also experienced issues relating to the MNO’s ownership of the SIM. Having cryptographic keys that enable secure access and identification for a bank’s Internet site stored in the MNO’s SIM is a sensitive issue.

To counter the ownership issues, some banks and MNOs have made trials using two SIMs (multi-slot) in the handheld device, one belonging to the MNO and one belonging to the Service Provider. This has meant modifications both for the hardware and software in the handheld device and is clearly not the best option for a future in which a large amount of different services will have to be offered quickly and securely to the end users.

The issues that have been discussed here become even more evident when designing services that extend over national boarders. However, voice services are already offered across national borders, and the same could (and should) happen for data services as well.

**Challenges facing the industry as a whole**

Rampant credit card fraud continues to weaken consumer confidence in online commerce and drive up the price of transactions. To combat this, many companies are now seeking to enhance security and add trust.

This raises several important issues:

- The need for consumer and retail industry awareness and adoption of the solutions available to address mobile security issues.
- Little or no standardization governing the security practices for establishing, registering, and validating the identity of transacting parties, especially when these parties are mobile and roam internationally.
- A plethora of “island solutions” in security emerging in the wired and wireless world, which is resulting in fragmentation and confusion among consumers, operators, service providers, and content providers.
- Lack of a uniform framework or common foundation for mobile business applications raises the cost of implementation.
- Legal issues surrounding liability (risk management), privacy rights, and the recognition of digital signatures in many countries are too complex for any one company or market sector to solve, especially when the market is global.
- Market development has been hindered by “gridlock” as mobile operators and banks jockey for position in the new economy.

Many of the challenges presented by roaming with voice services have already been met. Nevertheless, roaming with data services and transactions brings up another set of challenges, as mobile subscribers roam with wireless data services between different networks, countries, and services providers. For mobile e-commerce services to reach their true potential, it must be possible to exploit the main advantage of wireless devices – that of mobility. In many markets, these services will soon be in place. But the question that needs to be asked is: Will subscribers be able to roam with their data services as they already can with voice services?
There is clearly a need for a trusted network platform that would overcome the inherent weaknesses of the Internet itself when accessing it over a wireless device. The Transaction Roaming Platform (suggested by Radicchio in early 2002) would form the base for a global neutral network that builds consumer confidence, offers positive user experience, and ensures a wide array of attractive services across national boundaries.

Such a wireless trusted network would be responsible for establishing business architectures, clarifying liability issues, specifying technical standards, facing regulatory challenges, and building bridges to other trust networks. Many companies have been working with Public Key Infrastructures (PKIs) to generate trust by providing non-repudiable authentication. Since the required technologies already exist, Radicchio’s t2r efforts have been directed towards defining the business environment for the use of a reliable, interoperable trust framework on a global scale.

Objectives

The t2r Platform must meet the following objectives:

- **Global interoperability** – The need for interoperability between secure networks that extends across national boundaries to other secure networks. For example, a subscriber who is roaming in a foreign MNO’s network has to be able to access familiar services as securely as in their home network.

- **Secure network access** – This is a prerequisite for any service in any network. However, many networks (for example: 802.11b) are not considered secure enough today. In these networks, a third party could eavesdrop on the communication or data flow. Networks that rely on smart cards for network access (as is the case with GSM) are considered more secure, because the SIMs offer advanced cryptographic capabilities and tamper resistance.

- **Secure content access** – Once a consumer has been able to securely access their preferred network, different Service Providers want to make sure that only their appropriate customers can securely access the content/service on offer.

- **Reliable identification** – Just as in the real world, some businesses want to identify you before they serve you. Reliable identification systems are especially important when conducting mobile commerce or dealing with financial or private information.

- **Privacy management** – Relationships between consumers and businesses are sensitive and frequently involve the exchange of private information. Consequently, both parties have responsibilities with regard to handling this information. Here, we need a technology to secure the information exchange and to protect and enable management of the private information, wherever it is stored.

- **Convenience & benefits** – End-users will be offered a vast amount of services on a global basis. In some cases, data may have to be added, deleted, edited, or updated. This could cause inconvenience. For instance, when a subscriber changes his/her handset to
The first steps have been taken towards t2r

Following a feasibility study on the main concept of trusted transaction roaming, which was done by Secartis AG and Ernst&Young, the t2r project was presented to the leading mobile operators at the Carrier Summit held in March 2002 in Bandol, France. Operators present included Hutchinson 3G, mm02, MTN, Orange, Sonera, T-mobile, and Vodafone. The aim of this summit was to reach a consensus on the best way to develop a global framework for trusted mobile and wireless transactions. The feedback was encouraging, and Radicchio believes that this summit has signaled the start of global roaming for secure wireless transactions.

To ensure that the framework becomes truly global, Radicchio invited the GSM Association and the Liberty Alliance to present at the Operator Summit. Follow-on efforts and cooperation was established with other leading industry bodies, such as the European Telecommunication Standardization Institute (ETSI) and the ICT Standards Board.

Radicchio helped to set-up and now participates in a European Community (EC) part-funded research project that is further developing the t2r concept. This project started on 1st September 2002 and was due to be completed by 31st August 2003. The project comprised: Gemplus (project manager), Orange, Radicchio, SmartTrust, Ubizen, Vodafone. The project has reviewed and leveraged other work, such as ETSI STF on mobile signatures, and developed the business framework and ecosystem for mobile authentication and consent. t2r will allow different technologies and provide flexibility in identity service provision; further work will address risk and liability within the t2r architecture and the different roles.

The t2r innovation

The key innovation lies in a new architecture that adds a neutral entity to operate a global platform that will use the property of all the MNOs in an equal way. It will use their network infrastructure and their SIM – USIM cards globally, to create one secure network that can be linked to other secure networks. The architecture will unleash the capabilities of SIM – USIM cards for everyone’s needs.

Legal enforcement – The relationship between the business and the consumer should take place in a fair way. However, clear dispute resolution authority is required in disputes of any kind. This authority could differ depending on the nature of the service (for example, financial service versus health services). Furthermore, the trusted entity that will operate the proposed platform must obey strict laws and guidelines.

Today, each service provider has to go through each Mobile Network Operator (MNO) to reach the wireless subscribers. The SIM card can be used to enhance the security of these service offerings, but each solution is proprietary and involves a complex implementation process between the MNO and Service Provider (see Figure 2 on page 15).
benefit and serve as a common platform enabling content and service providers to reach mobile subscribers in a trusted environment (see Figure 3).

The t²r platform could solve existing business issues in the wireless data services market. It changes the way that Mobile Network Operators and Service Providers interact with each other as they offer data services to wireless subscribers. The business case is founded on a revenue sharing model that could be of mutual benefit to both Service Providers and Mobile Network Operators.

In today’s business environment, the MNO has to negotiate separately with each Service Provider to bring a new secure wireless service offering into place. This includes business model issues, technical solutions, and policies (such as whether or not adult content is allowed). In the proposed trusted network platform, the entity could take over this costly negotiation operation and offer a stable revenue sharing model to both parties. The MNO would receive revenues in proportion to how its network resources have been used to distribute the services to the subscribers. This should result in a gradual increase of the ARPU (Average Revenue Per User) for Mobile Network Operators.

It is currently somewhat difficult for Service Providers to offer services to wireless customers by relying on the security provided by smart cards in the mobile networks (GSM). The Service Provider has to enter into specific agreements with the MNO for each network that should carry its service. This is an extremely complicated and slow process, and frequently requires proprietary security solutions. If a Service Provider wants to reach wireless subscribers on a global basis, the process becomes even more complex and costly. Radicchio’s t²r proposal would enable any Service Provider to benefit from the underlying security infrastructure and access wireless subscribers on a global basis. This would simplify the complex process of providing secure, high-quality services to wireless customers, which is an important prerequisite for a better customer relationship. This revenue sharing model could offer the Service Providers the opportunity to reach the global mass of wireless subscribers and also reduce the set-up and implementation cost of its offering.

Various parties stand to save time and money by using independent entities to operate the proposed platform in a trusted global network. Furthermore, unleashing the security and privacy potential of smart cards will benefit all parties involved. Smart cards are widely recognized secure tokens and are already implemented within the European telecommunication and financial industries.

Since the operator of such an extensive platform will deal with so many different parties’ confidential information, it must be a neutral entity that is truly trusted and recognized by all the players in the data services market – such as financial institutions, MNOs, and companies that provide services, content, or technology. This neutral entity could operate the Global Identity Management on behalf of all GSM Mobile Network Operators.

Conclusions

Establishing a large trusted marketplace for mobile e-commerce is too complex, too expensive, and too risky for a single company to accomplish on its own. The roaming framework for trusted mobile services must be:

- **Open**: by building a common, neutral platform for global transaction roaming and 3rd party applications.
- **Trusted**: to build consumer confidence.
- **Managed**: to allow content and service providers to reach a large base of mobile subscribers with compelling content without losing control of the networks.

Clearly, such a challenge requires a great deal of coordination between the major players involved, especially the Mobile Network Operators (they have the subscribers and networks) and Services Providers, such as banks (they have the expertise for handling financial transactions). If the industry agrees to build an infrastructure based on the Radicchio t²r proposal, they could begin the task of installing confidence in the system. Mobile commerce will only become a normal part of everyday life if people know that they can rely on their business partners and are protected against fraud.

**Radicchio**

Launched in 1999, Radicchio seeks to unleash the tremendous potential of the market for wireless data services, such as mobile e-commerce and mobile e-government. Guided by a cross industry board of directors including EDS, Ericsson, Gemplus, Giesecke & Devrient, MTN, Smarttrust and Vodafone, Radicchio is the authority and industry voice for trusted networks in the mobile world.

Radicchio’s focus is “Trusted Transaction Roaming - t²r”. t²r defines an identity framework, which enables mobile operators, financial institutions, governments and other service providers to strongly identify the end-user via the user’s mobile device, and thereby lower the risk and cost of e-commerce services. It comprises transactions in a broad/general sense, for example, strong end-user identity could reduce the risk of charge back for merchants and could enable authenticated access to services such as corporate and government portals. The identification framework works across both national and network borders, even while outside the home operator's network.

For more information visit: www.radicchio.org
Who’s Listening on your WLAN?

By Dr. Peter Laackmann, Infineon Technologies AG

Today, wireless LAN solutions offer a broad spectrum of products for easy network installation and operation, making intra-building communication free and simple. But up until now, this freedom has taken its toll. The open WLAN systems that are ubiquitous now open the door for attackers who are carrying out their espionage and manipulations with very simple equipment. The most spectacular example is the so-called “WarDriving”, which involves the attackers moving through a city in order to grab and map all open WLAN systems.

Equipment

Most WLAN standards are derivatives of the IEEE802.11, operating at 5 Gigahertz (IEEE802.11a) or 2.4 Gigahertz (IEEE802.11b). As the 5 Gigahertz band has formerly been used in Europe for other services, the IEEE802.11b is much more established in European countries. In setting up a WLAN network, two main components are required.

First, an Access Point has to be installed. The Access Point acts like a hub in a commonly used wired network; normally it is equipped with a non-directional antenna so that clients from all directions may log in. On the client side, a WLAN interface is required. These interfaces are available in the form of PCMCIA cards, e.g. for temporary integration in notebooks, but also as PCI cards for permanent assembly in desktop computers. Some newer devices contain a USB or TCP/IP port, making them comparable to external modems.

Every WLAN interface has its own address just like a conventional LAN card, so that clients only get the data that is intended for them. In the hands of an attacker, some cards can be programmed to the so-called “promiscuous” mode, where every data package, even with other destinations, can be read by the interface. Most WLAN interfaces contain their own internal antenna, but
additionally an external antenna can be connected, allowing a higher data transmission range. These antennas are also recommended, if there is a high amount of absorbing material such as metal or bricks between sender and receiver. Attackers use external antennas too, mostly to increase the range of radio interception, but sometimes also for locating a specific WLAN access point, if several points are detected simultaneously.

One particular example, which drew some media attraction, was the use of the “Pringles” potato chip can as a directional antenna. The inside surface of his pipe-shaped can is covered with a metallic lining, which acts like a wave guide for the WLAN radio signals. Parabolic antennas have even been successfully tested for interception of WLAN signals over a range of 40 kilometers, so the argument that WLAN systems should normally only bridge 100 meters does not apply for attacks (see Figure 1).

**WarDriving**

It is said the term “WarDriving” is derived from the term “WarDialing”, which means that a large number of telephone lines are automatically scanned (dialed) and tested for service modem connections. “WarDriving” stands for a very fast and efficient way of scanning a territory, like a city or a large building, for open and unsecured WLAN access points. WarDriving equipment usually consists of a portable notebook PC, a PCMCIA WLAN interface card, and a GPS (global positioning system) receiver. On the notebook PC, a scan program such as “NetStumbler” is run, which automatically searches for WLAN access points in the surrounding area.

If an access point is found, the software automatically retrieves the navigation coordinates from the GPS receiver, and logs all data including type of network, position and signal strength in a log file (see Figure 2).

Later on, the attacker can evaluate the captured data using mapping software like “StumbVerter”. These tools convert the log files from a WarDriving event into a street map. On this map, the access points are graphically marked, including information about the signal strength and characteristics of the observed networks (see Figure 3 on page 20).

Even a new form of urban art has been observed, the so-called “WarChalking”. The WarChalking signs on building walls contain information about the networks used therein.

WarChalking is reportedly used to inform other WarDrivers about already characterized networks. Figure 4 (on page 20) explains the different symbols used.

**Counter measures**

The standard IEEE802.11b already includes basic security functionality. An active authentication (Shared Key Authentication) and data encryption (Wireless Equivalence Privacy - WEP) were designed to protect the connection from manipulation and espionage. If WEP is to be used, both access points and clients have to be provided with the encryption keys, a procedure which may turn out to be a “key management nightmare”.

Using WEP, the message to be sent over the WLAN first has to be appended with an integrity check vector (ICV). The receiver used to check if the message has been illegally altered during the transmission uses this value.

Both message and ICV are then encrypted using the algorithm RC4. Every cryptographic operation, also RC4, needs a key, which in this case is derived from a 40-bit long seed and an initialization vector (IV). Both values are fed as a starting value into a pseudo random number generator. This generator supplies the WLAN interface with as many key bits, as there are message bits. The encrypted message is then sent over the air to the receiver, where it is decrypted using the same, mirrored process.

The authentication of a transmitter against the receiver is carried out utilizing a challenge and response protocol. The access point can send an encrypted random value to the client, which is subsequently tested using the same key in the receiver, and vice versa. If the
value is identified to be the right one, both stations have the same, secret key.

**Still Insecure?**

Despite using encryption and authentication, a WLAN network may still be insecure. The generation of the initial vectors, that are crucial for efficient encryption, is not specified in IEEE802.11.

If the encryption is to be protected against attacks, the transmitter must make sure that for every message, a different initial vector is to be used. As some systems just contain a limited, ascending counter for this purpose, an attacker can wait for two messages being encrypted with the same vector. In a typical network with a lot of traffic, all vectors of a typical 24-bit counter are used up after only five hours, which is then identical to the timescale for a successful attack.

Some systems allow the use of conventional passwords instead of typing in the 40 bits in binaric mode. The password is then transformed into the 40-bit encryption key, which would be a nice solution if some systems would not cut the efficient key length down to only 21 bits during this conversion. But even if all 40 bits are used, there is still the probability for an attack via the so-called “brute force” attack method. The search for a 40-bit RC4 key only takes some weeks on modern desktop computers.

As a countermeasure, WEP has been augmented to 128-bit key length. In this scenario, 104 bits are used as the encryption key, and 24 bits are utilized for the initial vector. With this key length, a brute force attack should be nearly impossible for the next few years. But not all deficiencies have been corrected.

**New Problems**

In 2001, Shamir, Mantin and Fluhr published a paper describing attacks on WLAN encryption using a completely different methodology. It is well known that for the encryption method RC4, there are many so-called “weak keys”; specific combinations of bits that allow attackers to extract secret information. If such a “weak key” is used, an attacker gets hold of parts of the clear text, non-encrypted message. The first attack software, based on this effect, is “WEP Crack”; searching a network transmission for weak keys.

“AirSnort”, a professional piece of software, does the complete attack automatically, including the sniffing of 100 megabytes to one gigabyte of data, searching for weak keys, and finally extracting the clear text messages. On a frequently used WLAN system, “AirSnort” just has to be used for three to four hours.

**The Future**

The new standard IEEE802.11i will be equipped with a new protocol, increasing the security of WLAN systems by far. A temporary key is generated for a limited number of data transmission packets, so that an attacker cannot search a vast amount of data for weak keys, and also cannot use a compromised key for the eavesdropping of the complete network traffic.

The aged RC4 encryption method can be replaced by the new standard AES (Advanced encryption standard), which has recently been introduced as a new, worldwide, symmetrical encryption algorithm with a very high security level.

**Literature References**


Governments and passport manufacturers are facing unique challenges in trying to meet new requirements for preventing illegal immigration, international crime and terrorism, as well as supporting efficient border crossing of authorized passengers, especially frequent flyers. After September 11th 2001 there has also been pressure to develop security systems for border crossing authorities and the airline industry.

The means for security improvements have been looked for in many different systems, like online register controls and advance passenger information (API) systems at borders, and in technologies such as biometrics supporting new security requirements, which partly are also set by legislation and international agreements.

One of the key facilitators for security improvement will be travel documents in the form of passports, travel cards or visas. Biometrics has been widely recognized in this area as a technology for solving the problem of unreliable identification of persons accessing an authorized area (i.e. entering a country).

**A standard solution for international interoperability**

Technology enhancements in travel documents will only be seen as partial solutions if they are not adapted on a global scale. Together with the need to support traditional approaches, standardization for new technologies is necessary, otherwise there may well be delays in their deployment.

The leading authority for international interoperability of travel documents is ICAO, which in the late 80’s developed the standard for Machine Readable Travel Documents (MRTD), deploying OCR-B character recognition technology. Governments have adopted this technology slowly but widely, so that today the majority of countries are issuing MRTDs and deploying OCR-B in border control systems.

Even before the terrorist attacks, ICAO recognized that to ensure efficient and secure border crossing, there should be an added means to MRTDs for machine assisted person identification (i.e. biometrics for machine assisted document authentication).

This has necessitated the specification of co-existing technologies to MRTDs, in order to allow for additional storage capacity as well as more efficient access to data. As the standard storage technologies have been ID1-type card oriented, the only feasible technologies for passport booklets and visas (sticker) are limited to 2D-barcode and the contactless chip.

Another big problem that ICAO has been facing, is the immaturity of biometric technologies and markets. The market is currently fragmented and there are many different technologies competing for the dominant position. After a detailed evaluation process, ICAO is now on the way to specifying face recognition as an obligatory element of the travel document standards, together with optional fingerprint and iris recognition.

As the standardization of biometrics is in its early phase and the technical solutions are mainly proprietary, the result is the deployment of inefficient and generic biometric data formats in travel document standards. Together with other necessary data, the biometric data in practice needs so much space that it can’t be stored in 2D barcodes. So the only possible technology for biometric passports is a contactless chip with relatively large memory - at least 16kB.
Many innovative technologies, based for example on magnetic or optic recognition with different wavelengths of security elements and/or personalized data etc., have been developed for machine assisted document authentication and integrity verification. The problems with these technologies are again the proprietary solutions and the lack of mainstream solutions. These issues and the lack of feasible market entry mechanisms, are prohibiting the global deployment of such solutions. Luckily, implementation of a contactless chip as a passport storage media can allow secure deployment of Public Key Infrastructure (PKI) for document authentication and integrity verification. The focus is moving from the security of documents to the security of the issuance process i.e. to the reliable initial identification of the person and to the security and data integrity throughout the identification process until delivery of the document to the correct holder. This also sets new security and reliability demands for systems deployed in the issuance process. The security requirements are also putting pressure on centralizing the issuance and personalization processes.

Technology challenges

All the developing technology and security demands, as well as infrastructure challenges, mean a quantum leap for passport issuers and manufactures, especially for those deploying traditional technologies such as laminated data pages with distributed main stream printing technologies. This is especially true for vendors of governments willing to meet the standard set by the US Government for the Visa Waiver Program, requiring passports to adhere to the new ICAO biometrics standards as per October 26th 2004. The current situation requires new technologies to be implemented with very little proven experience. These models include the implementation of secure and durable contactless chips in passport booklets, the selection of the most feasible biometrics or a combination of multimode technologies. Other models include the implementation of enrollment, issuance, personalization and verification processes of biometric data and the implementation of border control processes and systems deploying biometric data, etc.

Security of documents and processes

The physical security of travel documents requires continuous improvement and there are different bodies defining the security requirements for documents, as well as for the issuing processes and systems. In addition to ICAO, the EU Commission by Minimum Travel Document Security Directive, for example, is taking care of security issues. When making decisions about document security requirements, the above-mentioned organizations utilize traditional security material, printing technology possibilities, obligatory optically variable devices (OVD) and image reproduction requirements. The focus is moving from the security of documents to the security of the issuance processes i.e. to the reliable initial identification of the person and to the security and data integrity throughout the identification process until delivery of the document to the correct holder. This also sets new security and reliability demands for systems deployed in the issuance process. The security requirements are also putting pressure on centralizing the issuance and personalization processes.

Contactless chips in biometric passports

The implementation of a chip in the passport book is one of the most critical challenges for the passport manufacturer. The chip with antenna can be placed on the data page, cover, or sandwiched between the center leaves. The key issue in implementation is the size of the chip. Because of the large memory requirements, the modules of the chips are large and thick, which causes problems when modules are attached to the data page with all the security elements. The thickness of the page, as well as the durability of the integration under physical stress, can become critical. The security risks arise from the possibility of separating a valid chip from one passport and attaching it to another document. The protection against tampering is very difficult in a construction where the chip is inside the cover or between the center pages. In these cases, recognizing a possible counterfeit is also extremely difficult. The data page is preferred because the chip can be most reliably integrated directly to the important personalized data, thereby maximizing the security. So far the most promising solutions include a chip integrated into plastic-based data pages made, for example, from polycarbonate with laser engraved visual personalization.

Until now, there have been no measures set by standards or best practices to validate the durability of the booklet with a chip and antenna. This together with chip durability limitations and the ageing problem of biometrics, especially of face recognition technology, seem to decrease the validity of the documents down from the usual 10 years. The selection of the chip type and memory size today, is partly limited by
the availability of feasible components. In principle, ordinary memory chips supporting ISO 14443 with enough storage could be a possibility, but in practice the security and direct access to large data areas require support of an ISO 7816 type Operating System. However, in the near future the market might supply up to 64kB chips with multi-application support in feasible modules.

Usage of advanced components allows the issuer to develop new business cases by marketing solutions based on the usage of PKI co-processor chips to airline companies and travel agents, for example, for e-commerce and e-ticketing. Without developing new business cases, the cost structure for the issuers might, in many cases, form a real obstacle for migration to biometric passports.

Selection of the most feasible biometrics or combination of multimode technologies

When implementing biometric passports, a lot of attention has to be focused on the selection of biometrics. In addition to the obligatory interoperable face presentation, the issuer has to decide whether to add one or more proprietary face templates, as well as interoperable fingerprint and/or iris presentations together with one or more templates. This decision also has to be coordinated with the national border control policy.

Until now, the support from biometrics research has been very limited when it comes to making decisions based on costs, reliability and convenience. In practice, the early implementation experience will show if the quality of the selection is adequate or if an adaptive approach is required.

Implementing enrollment, issuance, personalization and verification processes of biometric data

One of the greatest challenges for the issuer is the development of a nationwide system for the enrollment of biometrics. The solution should be convenient, non-intrusive, efficient and economical addition to the enrollment of application procedures. Centralization of the personalization process forms the most secure architecture for biometric passports and the verification of the reliability of biometric data and identification has to be ensured at some practical level.

Implementation of border control processes and systems deploying biometric data

The implementation of biometric passports cannot be effective if deployment is not planned at the same time. The interdependence of issuance, biometric passports and border control is very strong. With the expected global commitment to ISO 14443 type biometric passports, there remains the need to invest only in contactless readers connected directly or through self-service kiosks. Making decisions about identification and authentication software is somewhat complicated and it has to be adopted according to the risk levels and the market development of selected biometrics in passports.

Summary

The biometric passport market is starting to open up as a consequence of the up-coming standards. This also creates opportunities for all issuers; to benefit from each other’s investments by creating more secure passports and the related infrastructures.

The new basic technologies for passports already exist, but there is still a lot of development and research work to be done before being able to supply the issuers and users with qualified solutions that solve their unique needs and problems of identifying people with biometric passports at passport control.
Secure identification of individuals is a fundamental and critical function in any country. Events since 9/11 have increased national interests in implementing more secure personal ID systems, to improve confidence in verifying the identities of individuals seeking access to physical or virtual locations. This applies whether identification is needed at an immigration counter checkpoint, or at a government hosted web site offering citizen services.

Widespread use of information systems and Internet technology is revolutionizing the way governments and businesses communicate with and deliver services to citizens, providing cost, time and resource savings. However, this convergence towards an on-line adapted world has created new types of risks and challenges, that traditional ID cards issued by governments and enterprises are unable to solve due to their limited functionality capabilities.

Debates are taking place in many countries around the world, arguing the possibilities to issue a new type of ID in the form of a smart card, with or without some form of biometrics functionality, such as fingerprint recognition. The most commonly used argument against deployment of national ID cards, is the fear of compromising privacy and thus freedom of individuals. Civil liberty unions and privacy lobbyists claim that a national ID program would create a unique way for governments to track citizens, resulting in profiling and discrimination.

Smart cards provide a solution that brings a positive and innovative response to this current privacy debate, offering a number of advantages compared to any other form of ID document. Above all, the technology constitutes a strong and convincing case for reducing the continuing privacy concerns, by enabling the end-user to gain a high level of control of private identification data.

**Mobility and Off-line Capabilities**

Off-line verification is one of the strongest advantages that smart cards possess in comparison to other technologies. Through this feature, smart card-based identity verification can be cost-effectively deployed at the various physical security checkpoints that require validation of identity – for example, at different locations in an airport, a road control, or other security facilities.

Security officers can verify an individual’s identity by prompting an ID cardholder to enter his or her PIN (Personal
Application Focus

Identification

Identification Number) code, or by comparing a scanned biometric, such as a fingerprint, with a biometric stored on the card. This unique technology eliminates the need for on-line access to a central database by restricting the data shared to an individual entity, thus controlling citizen privacy. Furthermore, with its capacity to store, read, write and update information in a very secure environment, a smart card can easily be interconnected with multiple existing databases. This eliminates the need to link all these independent legacy systems, hence reducing the possibility of privacy infringement imposed by a unique government controlled citizen database.

Information Segregation

Along with the strong information protection and security that is inherent to smart card technology, a smart ID card is able to share ONLY the information required for a specific situation or location.

Firstly, the card content is protected against unauthorized access by a unique PIN code, and/or by the owner's fingerprint, and always stays in full possession of its owner. Furthermore, the card's unique ability to verify the authority of the information requestor allows it to be the perfect guardian of a citizen's personal information. All of the cardholder’s personal information does not need to be revealed every time in order to validate someone's identity. The information shared can vary depending on the specific “role” of the individual at a given point in time. I.e. only the data required for a defined identification purpose would be presented to the government authority in question. For example, to a police officer in a road control, a smart card will present information related to the motor vehicle authority (and this information may vary depending on the country or state issuing the license).

To a retail shop owner selling alcohol or tobacco, a smart card will only present information strictly related to the age of the ID cardholder, with no reference to the name and the address of the individual.

Consequently, by allowing authorized and authenticated access only to the information required during a governmental identification operation, a smart card-based ID card can effectively protect the citizen's privacy, while at the same time ensuring that the individual is properly identified.

Smart Driver’s License & Vehicle Registration Program

Since 1998, Gemplus has delivered smart card technology to the El Salvador government’s smart card program for driver’s license and vehicle registration. Through the use of smart cards, the system efficiently manages real-time vehicle and driver-related infractions and payments for the citizens of El Salvador. Over 2 million cards have already been issued to registered drivers of El Salvador, and 60,000 new cards are being issued every month (see Figure 1).

Smart Immigration Clearance Program

For nearly a decade, Gemplus has supported the Singapore government’s smart card-based Immigration Automated Clearance System. Smart cards are used to store the cardholder’s fingerprint for secure identification and automated immigration clearance of trans-border workers and frequent travellers at Singapore’s major points of entry. The smart card program has resulted in increased airport security as well as reduced immigration clearance time.

Smart Identification of Citizens

In 2002, Gemplus was selected to provide over 1.2 million smart cards to the Sultanate of Oman in order to streamline and increase quality of public services through an automated citizen ID system. Through the use of smart cards, Omani citizens and residents will be able to identify themselves at local authorities all over the country. The Oman national smart ID card program is the first ever smart card-based citizen identity solution to be deployed in the Middle East.

Smart Healthcare Insurance Cards

Since 1995 Gemplus has been providing smart cards and readers to the Slovenian government’s Healthcare Card program. All Slovenians are automatically issued a Health Insurance Card, which stores the cardholder’s medical data, such as organ donor status, prescriptions supplied and emergency medical data. Thus, during a patient visit, a physician can easily view the patient’s eligibility status and coverage status, as well as the primary physician designation.

Smart Driver’s License & Vehicle Registration Program

Smart Immigration Clearance Program

Smart Identification of Citizens

Smart Healthcare Insurance Cards

Identification Number) code, or by comparing a scanned biometric, such as a fingerprint, with a biometric stored on the card. This unique technology eliminates the need for on-line access to a central database by restricting the data shared to an individual entity, thus controlling citizen privacy. Furthermore, with its capacity to store, read, write and update information in a very secure environment, a smart card can easily be interconnected with multiple existing databases. This eliminates the need to link all these independent legacy systems, hence reducing the possibility of privacy infringement imposed by a unique government controlled citizen database.

Information Segregation

Along with the strong information protection and security that is inherent to smart card technology, a smart ID card is able to share ONLY the information required for a specific situation or location.

Firstly, the card content is protected against unauthorized access by a unique PIN code, and/or by the owner's fingerprint, and always stays in full possession of its owner. Furthermore, the card's unique ability to verify the authority of the information requestor allows it to be the perfect guardian of a citizen's personal information. All of the cardholder's personal information does not need to be revealed every time in order to validate someone's identity. The information shared can vary depending on the specific “role” of the individual at a given point in time. I.e. only the data required for a defined identification purpose would be presented to the government authority in question. For example, to a police officer in a road control, a smart card will present information related to the motor vehicle authority (and this information may vary depending on the country or state issuing the license).

To a retail shop owner selling alcohol or tobacco, a smart card will only present information strictly related to the age of the ID cardholder, with no reference to the name and the address of the individual.

Consequently, by allowing authorized and authenticated access only to the information required during a governmental identification operation, a smart card-based ID card can effectively protect the citizen's privacy, while at the same time ensuring that the individual is properly identified.

For more information visit: www.gemplus.com

Figure 1: Using a smart card to identify a driver
Smart Proof of Citizenship

By SC2

A National ID Card is a project that any company should enter into with a certain amount of caution. These projects tend to be fairly complicated, with many aspects that must be studied and carefully considered, in order to ensure unexpected problems are kept to a minimum and financial rewards are maximized.

The first issue that SC2 had to deal with was who, by definition, was the client? A client receives a company’s solutions and products and hence can measure their success. The National ID Card is a project where there are two major clients for one single project, both of which are extremely demanding. The first client is the Israeli government, who initiated the project and selected the solution providers. This client is very security and technology aware, which impacts their demands. The second "client" is the civilian population. It can be argued that they were not SC2’s direct clients, but the fact remains that the civilians are the ones who will make daily use of the end product. This means that even though SC2 would not be expected to interact directly with the second client, their characteristics and opinions are nevertheless important.

In order to fully understand the scope of this project, we should take a moment to review the background issues faced by the main client. Over time, methods have been developed to forge Israeli National IDs. This results in high costs caused by various forgery scams from different business layers and markets. The situation has prompted the Israeli government to embark on a project, which will bring such problems to an end. It is important to mention that this was not done over-night; prior to starting this project, a detailed process of legislation and preparation took place, in terms of digital signature laws, and governmental smart card and information security standards.

The “outputs” of this project can be divided into three stages: the physical part, the electrical part, and deployment. The physical stage includes the smart card material and manufacturing, visual anti-fraud solutions, and the visual personalization of the cards. The electrical stage includes the preparation of information for personalization and the actual electrical personalization. The deployment stage includes the distribution methods of the card from the factory, through the personalization process and into the hands of the users.

Physical Process

For this project, SC2 were asked to provide a smart card that will last with daily use, for a minimum of 5 years. The only plastic material capable of that today is polycarbonate. However, satisfying the durability demands was only half the solution. Having experienced many fraud and forgery issues, the Israeli government demanded the best, most advanced, anti-forgery solution currently available. To fulfill such a requirement, the SC2 solution includes various security elements. With such a combination, SC2 have been able to present an impossible-to-forge ID card.

Electrical Process

This stage includes the implementation of interfaces between data sources, the SC2 personalization systems and the actual writing of data onto the smart card. The SC2 personalization system is capable of connecting to various data sources through standard protocols such as SQL, ODBC, LDAP, etc. Using these connections, data (information about civilians, weapon licenses, driving licenses, topographic information etc.) is retrieved from governmental databases. The collected data is processed by the SC2 personalization system and then prepared for the actual personalization. (There is another connection to Certificate Authorities, but this one is usually only used during the actual personalization process, which will be described later on in this article.)
The actual personalization is in some ways the climax of the process. This is the stage where everything that has been previously prepared is implemented. The personalization system commands a smart card printer to pull a card from its input tray and begin the electrical personalization. This operation includes building a unique file structure, writing personal and governmental data, and the installation of digital certificates. A quality assurance procedure is performed immediately after the electrical personalization process, to verify the written data and once finished, the card is transferred to the printing position. Visual data is then printed onto the surface of the card. Printing is done in two ways; one is common thermal printing, and the other is laser-engraving printing. Both methods are used to eliminate the possibility of ID card forgery.

Before moving on to the distribution of the cards, we should look at two important subjects in a little more depth: the connection to Certificate Authorities and the smart card’s operating system itself.

Certificate Authority

The specification for this project required the ability to connect to external Certificate Authorities (CAs). The CAs are responsible for both issuing and signing the digital certificates stored on the ID card. The process of issuing digital certificates can be performed in two ways, and SC2 were required to support both. The first, and more secure way, is when a dual RSA key pair is generated inside the smart card, and the request for the digital certificate is sent to the CA using the Public Key from this specific key pair. Using this method, the Private Key is secured inside the smart card, and does not exist outside of the token. The second way is for the CA to generate the key pair, and send the digital certificate to the smart card along with the Private Key. Even though the CA is highly secure (as is the connection), it is still far more secure to generate the key pair actually inside the card itself.

Operating Systems

This leads us to consider the smart card operating system. The selected operating system for this project is the Apollo OS developed by SC2. The client took several important factors into consideration, in order to come to this specific OS selection. The Apollo OS has several unique features, which are extremely important for large-scale smart card projects:

- The ability to support both methods of the digital certificate issuance.
- An automated memory management module (part of the operating system) which provides a transparent memory management and defragmentation solution, releasing the client from the need to manually perform this task.
- Perhaps the most important feature, is the access security capabilities of the Apollo OS. Implementing a unique access protection mechanism, the Apollo OS provides the best security along with flexibility. Using the Apollo OS, we can define not only access conditions for certain identities, but also access rules that correlate between several of the authenticated identities.
- The capability to execute client proprietary applications on the card.
- And if this is not enough, the OS even supports the execution of both application and operating system patches and fixes.

Distribution

After reviewing both the personalization and operating system, the only remaining part of the process is the distribution of the cards to their end users - the civilians. The Israeli government only described their preferred distribution method in general terms, and left it to the provider to specify their detailed approach. The agreed distribution method has been decided as follows: Prior to the actual distribution, and parallel to the cards’ personalization, a transport user PIN is printed and sealed in an envelope when a card is personalized. At the end of the personalization process, two items are available: the ID card and the sealed PIN envelope. Each item is then sent separately (to ensure strict security) to the central branch of the Ministry of Internal Affairs (MoIF). The MoIF is then responsible for distributing the envelopes and the cards to its branches across the country. At those branches, when the card and the envelope are physically delivered into the hands of the civilians, the clerk sets the ID card status to “Active” in the management system, and a corresponding message is then sent to the CA to confirm the validity of the digital certificate when asked to.

Summary

SC2 is very familiar with demands for smart card solutions such as those described in this article. Our vast experience with these projects is one of the main forces that drove us to develop the Apollo OS into what it is today.

The only possible solution for projects such as National ID cards, Employee cards, Banking and Credit cards (and similar fields) are smart cards, which combine the most generic and flexible technology without compromising security in any way. The Apollo OS Smart Cards delivers such a complete solution and can be referred to more as a platform and an infrastructure, rather than another standard smart card operating system. It is important to remember that the Apollo OS smart card is only a part of the solution SC2 offers, including a key management server called “KMS2”, and our personalization system. Like many other clients, the Israeli government has understood that for its new National ID cards it has to work with the best technology and the most suitable company, which will be able to not only deliver the smart cards, but also develop and tailor specific solutions for an individual client’s needs.
The Card that Cares

By Michael Nitz, Giesecke & Devrient

Good health is everyone’s most precious asset. That’s why most of the countries in the world are concerned with their citizens’ well being. However, many of the world’s health care systems face a crisis. An electronic health card for patients is one proposed solution that would offer higher quality of care, increased efficiency, reduced costs and greater transparency.
The Future of Health Care

Glistening snow under blue skies and lots of sunshine — conditions that draw crowds of delighted skiers and snowboarders to the slopes. But all isn’t fun and games up on those mountains. Accidents are commonplace, and even experienced skiers sometimes take a tumble and find themselves rushed by helicopter to a hospital. In such emergencies the following scenario might soon be put into practice: Taking a patient health card (PHC) from the pocket of an unconscious accident victim, an emergency medical technician (EMT) inserts the card into a card reader containing the EMT’s health professional card (HPC), which is similar to a subscriber identity module (SIM) card. The paramedic then simply enters a PIN to access the emergency care information the health cardholder has preauthorized for release in such circumstances. Later in a nearby hospital, the recovering patient runs his or her card through a reading device and enters a PIN to bring up information such as the insurance number, name, address and medical data for the hospital staff. Physicians can also use their HPC and PIN to record treatment details on the patient health card.

The card also makes it easier to get prescriptions issued. Like the paramedic on the ski slope, pharmacists can use their HPCs and PINs to authenticate themselves to the PHC. They can then read out any non-issued prescriptions and delete them once the medications have been dispensed.

When a customer’s medication record is listed on his or her card, the pharmacist can examine it either immediately or after the customer has authorized it via a PIN, a feature that makes it possible to check for contradictions. This card technology replaces the traditional paper prescription with an e-prescription, which the prescribing doctor enters and signs electronically on the patient’s health card. In addition, the system uses the doctor’s e-signature to verify the authorization. At the next visit to the family doctor or specialist, the patient once again enters his health card and PIN and, depending on the card type and system version, the physician can view the hospital’s findings, X-rays and the patient’s prescription history. All of these advances are technically feasible. What is needed is the political will to implement the system.

Taiwan — Putting theory into practice

While experts in Germany are currently discussing various health insurance card models, Taiwan has already set up a modern and effective health card system that has replaced paper-based health services vouchers with multi-functional microprocessor cards. Giesecke & Devrient developed the Taiwan system, which is the world’s largest health card project based on an open platform, using Java technology. G&D, which is based in Munich, Germany, worked closely on the project with its Taiwanese partner Teco Electric & Machinery Co., Ltd. The project comprises more than 22 million health insurance cards, 345,000 health professional cards with a signature function for doctors, pharmacists and hospitals, as well as terminals equipped with security modules. Here, too, system users identify themselves with a PIN, and the system can be programmed for additional security mechanisms and functions. Gregor Boeckeler, G&D project manager for Taiwan, expects that more benefits are still to come. “Operators are not yet making full use of the system’s potential,” explains Boeckeler “and it will remain migration-capable in the future.”

“By introducing multifunctional microprocessor cards and health system reform, we expect to save approximately €195 million.” Lee Ming Liang, Taiwan Health Department Minister

TAIWAN

Population: 24 million
Health cardholders: 22.3 million
Citizen information: Ambitious campaign launched with timely, up-to-date information including; personal testimonials, comprehensive newspaper articles and magazine reports, plus radio and television time. Additional media will include advertisements, brochures, information and discussion events, as well as hotlines.

Source: Bureau of National Health Insurance, Taipei
Project duration: 18 months (from call for tenders to completed card distribution)
Health Care

Plans in Europe

In 2002, German Health Minister Ulla Schmidt joined the representatives of doctors, pharmacists and health insurance companies in agreeing that patients in Germany should be able to store additional data on their health insurance cards. The agreement will allow permanent information to be stored on the cards, such as crucial emergency medical data including blood groups. The first step will be to run some model tests. For electronic prescriptions, for example, doctors would be able to use computers to archive prescriptions on a server. Patients could then receive printouts, and pharmacists could use individual encryption to call up the information from their servers.

In pilot tests, conventional health insurance cards (like those carried by about 72 million Germans) were upgraded to include server access authorization. In an initial test jointly conducted by the German Health Ministry and the Association of Statutory Health Insurance Physicians in North Rhine-Westphalia, Germany, the microprocessor card passed with flying colors.

The testing covered features such as e-prescription, e-referral, e-hospitalization and the recall of emergency data. “The health card allows for secure electronic exchange of data throughout the health care system,” explains Dr. Leonhard Hansen, deputy president of the National Association of Statutory Health Insurance Physicians.

“\textit{The health card is an important step toward increasing the quality of the health care system.}” \textit{Ulla Schmidt, German Health Minister}

Health Minister Schmidt also emphasized the card’s benefits, calling it “An important step toward ensuring quality in the health care system.” The card technology can deliver on its quality-control claim because it reduces parallel treatment and increases transparency of medical care.

Switzerland also plans to introduce a mandatory, standardized insurance card. The plan’s first stage will involve streamlining administrative processes for policy-holders, insurers and health care providers in preparation for widespread use of the cards by 2005 or 2006.

In the second stage, the health card system will be implemented, becoming an electronic access key to an individual’s detailed health and medical treatment data. High on the list of Swiss expectations for the new program will be higher-quality treatment and lower costs, while at the same time stressing the need to safeguard each cardholder’s sensitive personal data.

Anne Eckart of the consulting firm Basler and Hofmann AG based in Zurich, Switzerland, fears that the general population will not readily accept the health insurance card solution. She reached the conclusion following a technology impact assessment study conducted by the Swiss Science and Technology Council, based in Bern. Eckart recommends a centralized institute for Switzerland, that could serve as an information and co-ordination hub for initiatives studying computer-based patient records.

In Germany, Health Minister Schmidt doesn’t share concerns that card technology will endanger privacy: “The electronic health care card allows us to strengthen the rights of patients. They can decide whether additional information may be stored on their new chip card, and they can also view information that previously was difficult or impossible to access.” Schmidt considers a so-called “blind box ” or “strong box” to be absolutely essential for data protection.

The feature would allow patients to store information they would prefer not to share with certain doctors, information on medications such as Viagra, methadone or HIV medication, for example. Schmidt also feels that introducing the electronic health card would demand a uniform IT architecture. And while the technical standards exist, the obligatory content has not yet been defined for Germany.

For more information visit: \url{www.gi-de.com}
Every smart card equipped with a microcontroller contains hardware-implemented software (e.g. the card operating system) as well as applications. The introduction of more powerful technologies and smaller chip structures allows the storage of this software not only in fixed ROM masks (Read Only Memory), but also in re-writable Flash memories. The public discussion about the advantages and disadvantages of these two alternatives today is very controversial; however, an exact security based examination delivers amazing results.


ROM-Memory

Most smart card controllers today are equipped with ROM (Read Only Memory). On a “Metal-ROM”, the information or program code is stored as a sequence of thin metal contacts. Another possibility is the so-called ‘Implantation-ROM’. In this instance, the information is coded into the substrate of the memory cells by a powerful ion beam.

ROM-Memory does not allow for deletion, nor can it be overwritten by the user via program commands. Therefore, all programs and data supposed to be in the ROM have to be installed through the production process. This is done using a “ROM-Mask” which contains all data and is used during the processing of the silicon chip. At first sight, the limitation of the irreversible writing process seems to be a disadvantage. But it also discourages potential attackers to modify the program code on less-secure chip cards.

First, grinding the surface of the memory with diamond dust and subsequently using an imaging method, can easily help visualization of the memory content of Implantation-ROM, as well as of Metal-ROM. On a Metal-ROM the connections can be identified directly by optical inspection, but for the Implantation-ROM a short-term etching process using special chemicals has to be used first. After this procedure, the ROM-content can easily be read under a microscope with the naked eye or, for larger data, with an automatic optical processing method (see Figure 1).

Another alternative would be to contact the wires connecting the memory with the heart of the chip card; the CPU. These wires carry the content of the memory that is currently processed by the CPU. Contacts to these wires can be established using “probing” methodology [2].

The selection of the separately used memory does not act as protection, as today, attacks aimed at reading different kinds of memories are available. This will later be shown on the example of Flash and EEPROM memories.

As well as all other kinds of memory, the ROM content has to be protected not only on the chip itself, but also during the transfer of the program code from the customer to the chip manufacturer during the manufacturing of the masks, as well as in the production process itself. Infineon utilizes a highly efficient and secure method in which the mask information is always encrypted, even on the chip itself. This ensures the security of the information even if an attacker visualizes the whole ROM structure on the chip, as they would only yield encrypted data which is useless to them.

Furthermore, Infineon offers a very convenient process for customers when both transferring ROM information encrypted and protected to Infineon production sites and verifying the encrypted data. Infineon has developed a process called SecureX and uses state-of-the-art cryptography. Encrypted in this way, even the most sensitive data can be put confidentially onto the ROM-Mask. The first time the chip is allowed to transform the encrypted data to clear text is during operation. But even then, only the clear text data is processed in the very heart of the microprocessor (the CPU core) which is protected against multiple attacks. Even the information that is transferred over the various bus-systems is encrypted.

Flash Memory

Flash memory can be compared to the commonly used EEPROM-Memory (Electrically Erasable Programmable Read Only Memory), which can be found in almost all current chip card controllers. The information is coded into each memory cell by imprinting electrons that subsequently are “caught”
in that place, enabling them to store the information for years. Flash memories allow deletion or reprogramming of any stored information. Higher voltages than the usual operating voltage of the smart card are needed to program EEPROM or Flash-ROM, which are not normally delivered by the smart card terminal. Therefore, these voltages have to be generated within the chip itself.

Today, Flash smart cards play an important role in the illegal sector, as attackers are using the feature of reprogramming the flash memory content. For example, one smart card equipped with a Flash controller that is freely available over the internet can be used to simulate original Pay-TV cards: Instead of the original Pay-TV card, the so-called “Funcard” is put into the Pay-TV decoder (see Figure 2).

On the other hand, only a few original cards with Flash memory can be found in this sector. The reprogramming option of the flash memory for currently available (and insufficiently protected) concepts allows attackers to change or delete security checks, protection mechanisms and operating time limitations just as they wish. Therefore, this particular sector prefers today’s ROM-based cards. This example clearly shows that if Flash memories are used as carriers for operating systems, highly effective security concepts have to be used to make sure that such a product cannot be modified or rewritten by attackers.

As is the case for ROM memories, the content of unsecured Flash memories may also be easily read. Signal lines can be contacted to scan the data traffic. If the memory is not protected by strong encryption, the attacker can get access to secret data stored therein. Today, different methods are known that can be used to directly read the content of Flash and EEPROM memory cells [3]. Even methods from other branches of chip analysis such as LIVA (Light Induced Voltage Alteration) can be used [4]. Another very effective possibility has emerged from the new attack method “Optical Induced Fault Attack” [5]. Additionally, a problem may arise after deleting Flash as well as EEPROM memory cells – maybe due to an alert – because there may still be “residues” of the previously stored information [6] and in some special cases, this residual information may be retrieved. So it can be assumed that attackers with appropriate methodologies are able to read ROM as well as Flash memory contents.

However, in some aspects, flash memory appears to be more sensitive against manipulation of content than ROM. The reason for this, is simply that the information is not stored in hard-wired metal lines, but as an amount of normally freely movable electrons. Unwanted changes in the memory content can take place if the Flash memory is exposed to high temperature or high radiation. Attackers can use these effects if no appropriate protection measures are implemented. Figure 3 summarizes the different attacks carried out against both technologies and provides some of the countermeasures available.

The Solution: High Security Flash Controller

Chip card controllers that are insufficiently protected – no matter if Flash or ROM is used – may be attacked via their memory. With the introduction of Flash products in the market, the attacks that were already successful in previous experiments are now moving to these products. Therefore, the authors, as a result of security examinations, would conclude that Flash cards have their place in storing memory for sensitive applications but only if they use integral security. Chip cards utilizing Flash memory have to be protected against attacks at least as well as those equipped with ROM. Both of these requirements are met through the use of Infineon’s integral security concept. The first barrier against an attacker is the active shield, covering the whole
chip. This ‘intelligent fence’ consists of an extremely narrow parallel structure of small metal wires with a distance of approximately one micron. Its wires are permanently driven with different random numbers. If these numbers do not reach the end of the active shield untouched, the chip recognizes that an intruder has tried to modify the chip hardware. If this happens, the chip triggers an alarm and the running program is instantly deactivated. The active shield is a very effective protection against many kinds of physical attacks, but for increased protection of the memory, a number of further barriers are implemented. One of the most important protection measures is the strong memory encryption through an MED (Memory Encryption Decryption Unit). It makes sure that an attacker, even if he can directly read the Flash memory), can only get unusable encrypted values. So the attacker cannot understand the program and secret data contained within, nor can they manipulate this data because the attacker does not know how a specific command is to be encrypted. Even if they try to delete the whole Flash memory, the attacker will still not get any usable data, as a special system protects against reprogramming. Authorized changes of the Flash memory in the field through legal users however, are still possible.

Using strong memory encryption, as well as numerous other components of the integral security concept, all types of memory technologies implemented on a chip can be efficiently protected. The features of the memory itself are only of less importance.

Infineon’s first pure Flash-Security-Controller is the SLE88CFX4000P. Engineering Samples of this highly interesting device are planned to be available by end of 2003. The positive feedback from Infineon’s customers regarding this concept shows that Flash-Security-Controllers equipped with adequate integral security will have a very strong impact on the smart card market. Even the fear that Flash-Security-Controllers may not be suitable for high-volume applications because of higher costs can be countered - the SLE88CFX4000P has been specially designed to meet the requirements of mass markets and will therefore allow a cost-efficient implementation in all market segments.

Therefore it is possible to create not only pilot lots – for customer internal tests or field trials – at the push of a button, but also to start high volume production immediately after the evaluation phase using the same device. Likewise, logistics will be simplified as the same smart card controller is configurable for several applications. Altogether, the concept of a secure Flash smart card controller offers the option to apply security applications on Flash controllers for the first time.

The challenge to compete against an upcoming attack technology, and to successfully defend intrusions, is the central motivation for the development of new security controllers. Until today, numerous countermeasures have been developed and tested with simulated and real attacks. By nature, the research does not stagnate in this particular section. The development of new technologies for attacks spurs on the conception and realization of new counter-measures and the evaluation of methods for the testing of security functions. Proactive thinking allows us to recognize attacks of the future and to integrate security features against future threats today.

**Figure 3: Attacks and Countermeasures for Flash and ROM memories**

<table>
<thead>
<tr>
<th>Attack</th>
<th>Against ROM</th>
<th>Against Flash</th>
<th>Countermeasures (examples)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probing (Needle attacks, FIB)</td>
<td>Relatively easy</td>
<td>Relatively easy</td>
<td>Memory encryption, Active shield, Bus encryption</td>
</tr>
<tr>
<td>Forcing (Needle attacks, FIB)</td>
<td>Relatively easy</td>
<td>Relatively easy</td>
<td>Memory encryption, Active shield, Bus encryption</td>
</tr>
<tr>
<td>Visualization</td>
<td>Relatively easy</td>
<td>Relatively difficult</td>
<td>Memory encryption</td>
</tr>
<tr>
<td>Erasing</td>
<td>Relatively difficult</td>
<td>Relatively easy</td>
<td>Memory encryption, Error correction</td>
</tr>
<tr>
<td>Optical Induced Fault Attacks</td>
<td>Relatively easy</td>
<td>Relatively easy</td>
<td>Memory encryption, Error correction, Light sensors</td>
</tr>
<tr>
<td>Power Analysis</td>
<td>Relatively easy</td>
<td>Relatively easy</td>
<td>Memory encryption, Error correction, Bus encryption</td>
</tr>
<tr>
<td>Attacks using radiation</td>
<td>Relatively difficult</td>
<td>Relatively easy</td>
<td>Memory encryption, Error correction</td>
</tr>
<tr>
<td>Differential Fault Analysis (DFA)</td>
<td>Relatively easy</td>
<td>Relatively easy</td>
<td>Memory encryption, Error correction, Bus encryption</td>
</tr>
</tbody>
</table>

**Literature References**


Single Event Effects – Security Controllers under Attack

By Marcus Janke, Dr. Peter Laackmann

Nuclear radiation is known to not only be harmful to human beings, but also pose a significant threat to the functionality and security of microcontrollers. In the area of aerospace electronics, the effects of radiation on electronic systems are well documented and have been investigated for many years [1,2]. The reason for these intense efforts is the fact that under space conditions, nuclear radiation is much higher than on the earth’s surface and one single failure in a spacecraft’s electronics could mean the loss of millions of dollars.
A very common phenomenon in this area is the so-called “Single Event Effect” (SEE). If a semiconductor device is being hit by an atomic particle with a very high energy, for a particularly short time period, a conductive channel in the device is created.

This conductive channel can be compared to a short-circuit, but as it is located only in a very small sub-micron area, it will not in most cases damage the chip permanently, nor even cause a complete dysfunction. But it can – and sometimes will – cause faults in the operation of the device [3] that can be harmful to security (see Figure 1).

A particularly efficient way of generating Single Event Effects is to use ions with a very high energy, such as alpha particles, that consist of a helium atom without its electrons. For the occurrence of Single Event Effects, it is very important that the particles lose a high amount of their energy in a very small area inside the device. All this energy is thereby transferred to the surrounding silicon, so that the conductive channel can be set up properly.

A well-known source for alpha particles with high energy is the metal Radium, which has in the past been used for luminous clock dials. In this example, its emitted alpha particles are shot onto a substance that is stimulated to emit the typical green glow-in-the-dark effect. For technical applications that demand alpha radiation, today the cheaper transuranium metal “Americium” is used, which can easily be produced from plutonium.

What is not so well known, is that several minerals also constantly emit alpha particles, including different ores and building materials. In the electronics industry, lead is not only known for posing an environmental risk, but also as an alpha particle emitter (just like boron). So for radiation-sensitive electronic devices, there are several “low-alpha-compounds” available today, that are reduced in composition in terms of these critical components [4].

**Attacks against Security Controllers**

Similar to attacks using visible light [5], an attacker could use Single Event Effects based calculation faults in a security controller for different purposes. One target, is to alter the normal program code sequence that the controller is working on at the moment. With such an attack, security tests like a PIN-comparison or the integrity test of (error-) counters could be manipulated. But more significantly, the correct reading of account values, debit counters or key information can be compromised.

If errors using alpha radiation are to be used in the DFA (Differential Fault Analysis) methodology, information about the secret keys may also be retrieved. In the worst case, using just one faulty computation, the complete secret key may be discovered by the attacker – and this faulty computation can be induced by just one single alpha particle hitting the security controller.

The observed effects are very similar to those being introduced by optical radiation: the functions normally taking place in the irradiated parts of the microcontroller are thereby manipulated.

But alpha radiation is not so easily controlled, unlike light. Due to their nature, the atoms (which a radioactive material such as radium consists of) emit alpha particles in a random fashion. Only the average rate of alpha particles per second is known (as the unit “Bequerel”). But neither the time point nor the impact area of every alpha particle can be predicted.
very high-energy rates of the alpha particles that modify the crystal structure of the silicon itself.

But there are also some advantages to using irradiation as an attack method: through perforating a simple aluminum foil, a very efficient mask can be produced for local irradiation of small areas on the security controller, such as memory or crypto modules.

Another advantage is the low detection of single alpha particles. Whereas irradiation with light can be detected relatively easily by means of optical sensors, the detection of alpha particles is much more complicated. Sensors on the chip itself are able to detect alpha particles under certain circumstances, but not every incoming alpha particle would cause an alarm. Also, a protective coating on the chip itself is not efficient, as very thin metallic structures can be penetrated by alpha particles relatively easily.

Using radiation as a hypothetical medium for cryptographic attacks has already been proposed by Quisquater [6], but no practical experiments or concrete results are publicly known. The first practical tests were performed some time ago at Infineon Technologies. In order to show if a malfunction in a security controller could be induced using alpha particles, and to see if the attack could be detected, a radioactive source containing a small amount of Radium-226 was used.

Infineon tested unsecured microcontrollers, as well as their security controllers. These products were irradiated directly, without the plastic chip cover that is normally part of a smart card. As the range of alpha particles in air is only one to two centimeters, the radioactive source was placed directly over the chip surface (see Figure 2). Under these conditions, the alpha particles could penetrate the silicon down to the active regions of the semiconductor material, transferring their complete energy to the surrounding silicon.

The complete area of the chip was irradiated in order to observe and understand as many of the effects as possible. On average, all areas of the chips were subject to the same dose rate of radiation.

What Infineon expected, was that using a radioactive source of appropriate strength, a significant amount of radiation-induced effects could be observed.

Whereas the standard microcontrollers were defenseless against the attack, the countermeasures utilized in the Infineon security controllers showed their effectiveness in detecting the attacks. This was not only due to the utilization of the internal sensors of the highly developed security controllers, but also the hardware-based surveillance measures of the CPU and memory modules in the chip itself. As well as the 16-Bit SLE66P, the new 32-Bit Security Controllers were also subjected to the tests.

The concept of integral security used in the Infineon Security Controllers...
was shown to be very efficient against the new attacks through the use of alpha particle radiation. This is not very surprising however, as the principle of such attacks had been considered during the development of DFA (Differential Fault Attack) countermeasures from the very beginning. Today, highly efficient barriers against these attacks are available through the use of Infineon products. Such an integral security concept supplies protecting functionalities today, against the attacks of tomorrow. Once again, the advantages of a proprietary CPU core, whose development has included security and performance from the very start, can clearly be demonstrated.

**Hi-Tech or Low-Tech, Attack?**

A first glance, attacks using particle radiation seem to be a high tech approach that can only be carried out in a special laboratory. But alpha emitters of appropriate strength can be found in several devices around today. Attackers can also utilize sources like old radium dials, which contain the radioactive material Radium-226 in significant amounts [7], for inducing errors in unsecured microcontrollers (see Figures 3). Other sources of alpha radiation are mantles for gas lanterns containing Thorium-232, or from smoke detectors containing Americium-241. Even if these sources (if properly used) are not a threat to health, they could pose a security threat if used by an attacker to manipulate a microcontroller (see Figure 4).

Also, it should be noted that not only alpha particles might cause faults in security relevant devices, but also X-rays, electrons (beta radiation) or neutrons. Nevertheless, single event attacks are best performed using alpha particles due to their high energy and very high-energy transfer rates in the silicon.

**Perspective**

The challenge of counteracting a rapidly growing wave of the most different attack scenarios, is a central point in the development of security controllers at Infineon Technologies.

Infineon has considered the methodology of DFA (Differential Fault Analysis), including the attacks using radioactive sources detailed above, for many years. Up until now, a huge variety of countermeasures has been developed, carried out and verified in the most demanding tests. But the research cannot stop, as new attack methods are also developed every day [8], which implies that the search for new security concepts must also continue. Forward thinking and implementation allows the company to identify the attack scenarios that may come tomorrow and to implement the necessary countermeasures today.

**Literature References**


Within the Trust

BIOPASSPORT®
Enterprise Server
The Biometric Solution for
Comprehensive Network Security

There are two main objectives for deploying biometrics in an enterprise: massive cost savings and a dramatic increase in IT-security. The administration of classic passwords is generally recognized to cost an organization at least € 350 per member of staff per year (Source: Gartner Group Study), while at the same time IT-security has also become a major concern. Official crime statistics throughout the world show significant increases of identity theft and computer espionage.

Only biometrics ensures that a person is really the person he or she purports to be. IdentAlink’s BioPassport Enterprise Server Family of products incorporates multi-layered biometrics, including IdentAlink’s proprietary finger recognition algorithms and high level encryption, that are combined with PKI to provide a convenient single sign-on structure for small to large scale organizations.

What is more, customers do not need any additional hardware to run the application. This is due to the fact that the application is built to be platform independent, which means that there will be no need to modify any existing infrastructure. For Windows® 2000/2003 networks it is essentially an Active Directory Plug-In. The Java 2 Enterprise Edition will be deployed to support Non-Windows or multiple networks, as well as for the provision of PKI.

IdentAlink’s BioPassport Enterprise Server includes multilayered biometrics (face and finger as standard – others on demand). In the case of finger recognition, there are various different sensors compliant with the software. The number of users, as well as domains, is not limited at all. PKI, including Digital Signature, is also integrated into the package.

It features True Single Sign On, central control of all infrastructures and complies with the European Data Protection Act. The IdentAlink solution supports all currently available sensors.

The BioPassport Enterprise Server
The BioPassport Enterprise Server contains the following modules:

- **BioPassport® BioLogon**
  This enables a user to login from a Windows® 2000 or XP workstation into any Windows, Linux- or Solaris-Network with chosen biometrics instead of a password.

- **BioPassport® Secure Application**
  This module allows all password-based applications (locally, on a network or even web based) to be secured with any chosen biometrics. This solution is available as a ready-to-use module that works with almost any ERP, QRM and Database Solutions on the market or as an SDK to be integrated into a proprietary application.

- **BioPassport® Secure Communication**
  This enables a user to send and receive digitally signed and encrypted e-mails including attachments, only when the user has been biometrically verified. It is provided as a Plug-In for MS Outlook® or as an SDK to be integrated in any other mail application. It also uses PKI with minimum 512 bit RSA and includes Digital Signature.

- **BioPassport® Time & Attendance (SDK)**
  Interfacing to all current Time & Attendance software

- **BioPassport® Physical Access Control (SDK)**
  Interfaces embedded units into BioPassport Enterprise Server.

- **BioPassport® Content Provider (SDK)**
  This enables any web-based content (Online Shopping, Online Banking) that is currently secured with a password to be protected with biometrics.

IdentAlink has also recently released standalone versions of its BioPassport Enterprise Server Family of products for small businesses and standalone computers.

For more information visit: www.identalink.com
Multos Products for Migration and Security

Keycorp Limited is a global leader in secure transaction products including: smart card operating systems; payment terminals for fixed, mobile and Internet applications; and e-commerce gateways.

Keycorp’s MULTOS, a secure, multi-application smart card operating system, is the pre-eminent smart card platform for EMV migration, secure identity and data security applications.

Two key market drivers have emerged for multi-application smart cards, that are proving to be consistent on a global scale; namely EMV migration and security.

EMV migration is the upgrading of existing magnetic-strip-based financial credit and debit cards to chip-based cards, in order to reduce fraud and increase the number of functions the card is capable of performing. This initiative has been led by the major card brands.

Market drivers for security, are based around the need to ensure the integrity of personal and business data, to enable such activities as access control or identification, data exchange, and data security.

This market includes such applications as national ID cards, contactless transport systems, PKI (Public Key Infrastructure) systems for e-business exchanges, and access control to physical or logical facilities. Governments have been leading some of the larger projects including the Hong Kong SMARTICS (smart card Identification System) card and the US Department of Defense, Common Access Card (CAC). These projects are utilizing the security and ease-of-use offered by smart cards to manage cardholder identity efficiently and with high integrity.

But what are the key requirements that a smart card must meet for successful implementation in any of these markets? In the majority of cases these include:

- Security of data: such as applications, cryptographic keys and manufacturing process
- Assurance of system components: only achievable through a truly open platform
- Cost effective, easy to use and easy to implement
- Ability to add/modify functionality in the future without compromising the solution
- Reduced risk by using proven technology that fits its purpose.

With these requirements in mind, the MULTOS smart card platform has become the predominant card operating system deployed today. MULTOS is an open-platform operating system that provides high security, high assurance and multiple applications for smart cards. MULTOS is unique in that it defines the complete smart card lifecycle including: the operating-system and APIs (Application Programming Interface), mechanisms for securely loading and deleting applications, security requirements for hardware and software, key management principles, and card personalization. The MULTOS business model is issuer-centric and as such, it is the issuer that controls which applications are loaded, which vendors to use and how much of the smart card project it wants to control.

Questions and Answers

What about security?
The Keycorp MULTOS product has been certified to ITSEC E6 – the highest level of security available for any multi-application smart card operating system. The platform includes a cryptographic chip providing the high security exchanges necessary for payments and PKI.

Is it a proven product?
MULTOS has proven field performance from financial applications to national ID projects, with over 20 million products deployed to date.

Who’s in control?
MULTOS is a fully open, issuer-centric scheme, allowing for complete choice of vendors in each stage of the process, right up to how much of the process the issuer wants to control. Applications can even be loaded or deleted after the cards have been issued.

What is the added value?
The flexibility of a multi-application platform means that several different value-added services can be offered to each customer. The Keycorp MULTOS module comes with the industry’s most widely used applications pre-loaded – EMV payment application, e-purse, PKI and biometrics (from Precise Biometrics). This leaves memory for customer specific applications.

What about support?
Keycorp and the MULTOS community have been developing and implementing successful smart card projects for many years. There are dozens of vendors in card manufacturing, personalization bureaus, application developers and off-the-shelf applications including EMV payments, e-purse, loyalty, ID, health, biometrics, PKI, contactless transport ticketing and others.

Keycorp offers MULTOS products on Infineon SLE66CX series silicon with 16K, 32K and 64K memory.
Explaining the SyntiQ Solution

SyntiQ International focuses on solutions for remotely controlled payment terminals and ATMs, that benefit retailers, terminal managers and software houses. SyntiQ began as a project within Interpay (the payment processor for the Netherlands), formally becoming an independent entity on July 1st, 2001.

The SyntiQ-Pay chip

The SyntiQ Solution is an integrated suite of both hardware and software. The core of the solution is the SyntiQ-Pay chip: a very small computer implemented on a single platform, the size of a SIM-card (as used in mobile phones and payment terminals). In essence, the SyntiQ Solution is the card device. It contains the full banking environment and uses the peripherals of its host, such as a printer, display and keyboard.

Almost all terminals installed and sold worldwide over the last few years contain an ISO (ID-000) slot, where the SyntiQ-Pay chip can be inserted. Although initially designed for payment terminals, the SyntiQ-Pay chip can also be used for ATMs, Mobile Phones, Personal Digital Assistants, Personal Computers and Set-top boxes.

Key Characteristics of the SyntiQ-Pay Solution

The SyntiQ Solution allows the user to develop one application for a new product or a product change, independent of the different card devices, device configurations and ATMs. The new applications can be downloaded remotely into card devices. The SyntiQ-Pay chip contains a Multos-based security microcontroller, which prevents the necessity of using SAMs (Secure Access Module) and enables the remote change of security functions and security keys in both devices.

Using the SyntiQ-Pay chip

The SyntiQ-Pay Chip can be inserted into existing card devices. Alternatively, a card device designed with a SyntiQ-Pay chip at the core can utilize the SyntiQ advantages to an even greater degree.

About SyntiQ International

SyntiQ International is dedicated to creating intelligent business solutions by using the possibilities of integrated information and communication technology. Based in the Netherlands and founded by Dutch banks and Interpay, SyntiQ has broadened its base by establishing strategic alliances worldwide. The company’s SyntiQ-Pay solution contains a complete payment environment that can be remotely controlled in a secure fashion and fits into all kinds of payment terminals.

For more information visit: www.syntiq.com
realtime Security in Brevard County

realtime North America enables SAP users to remove an accepted, but severely flawed, security practice!

The company realtime North America, Inc. is the progressive affiliate of the established European SAP consulting and software firm, realtime AG. realtime AG is an SAP solution house, established in 1986 in Europe and still managed by former senior SAP employees. The company has a client base of over 200 “Fortune Global 500” customers in Europe and North America including Bayer, DaimlerChrysler, Siemens, Toyota, Esso, Procter & Gamble, DuPont, Black & Decker, Nestlé, and others.

SAP recently presented bioLock at their annual Sapphire conference in Orlando, Florida as part of its homeland security effort. Additionally, SAP has installed and is displaying bioLock in their Global Solution Center in Pennsylvania. SAP is also rolling out a promotion of bioLock to the SAP sales team focusing on government sales.

Thomas Neudenberger, COO of realtime North America, states that “The function of bioLock is in providing a secure and convenient alternative to the insecure password-method of limiting access to valuable or sensitive data in IT systems”. Additionally according to Neudenberger, bioLock is “basic security” that every company should already have, and will have two years from now.

To utilize fingerprint technology combined with smart cards and RFID, realtime has partnered with the industry leading keyboard manufacturer, Cherry. Cherry provides their well-known keyboards with the award winning capacitive Infineon fingerprint sensor, plus smart card and RFID readers.
Within the Trust

bioLock – the choice of local government

A recent installation of bioLock was at Brevard County (Government) in Florida, providing much needed extra security. Brevard County Systems Supervisor, Rick Meshberger says he chose bioLock because the county needed to have secure single sign-on to multiple systems, the provision of extra security for access to sensitive information in the HR systems, to assist in compliance with the federal HIPAA standards and to provide access control to purchasing functions for the Emergency Management Effort. Because of the need to access multiple critical systems, 8-digit passwords with lower case, upper case and numbers were inconvenient, insecure, and time consuming to retrieve from PDAs where they were typically stored and secured with another easier-to-remember single password. Most importantly, Brevard County (which includes the city of Melbourne and the NASA space facilities at Cape Kennedy and Cape Canaveral, and lies in a hurricane prone area) needed to provide extra-secure access to emergency preparedness supplies that are necessary to protect an area of national importance. The large quantities of emergency supplies necessary for national security of the space launch areas can involve very large expenditures. Brevard operates its emergency preparedness command headquarters from an underground bunker capable of withstanding a nuclear blast, and needed comparable IT security to protect their systems.

Pete Gunn, Director of Safety and Security introduced realtime to the Brevard County leadership for the Florida Space Authority. Pete Gunn had learned of the benefits of bioLock, knew that Brevard County was looking for additional security, and immediately recognized the benefits that bioLock would have for an area so concerned with national security.

Other products from realtime

In addition to bioLock, realtime is a market leader with its Authorization Profile Management Tool for SAP called APM. APM has been installed over 150 times within Europe, and Fortune 500 companies and other clients benefit from its time savings compared to the SAP profile generator, as well as APM’s wide ranging auditing functions.

And, as Klaus-Dieter Janzon, EnBW (one of Europe’s largest energy companies) enthuses: "Utilizing the new role-based features of APM has enabled us to save 60% of our initial efforts to set up user profiles in SAP. But the benefits of APM haven’t stopped there. Thanks to other APM features (such as trace analysis and derived roles) we are currently experiencing a reduction of an additional 30-40% in our routine user and profile maintenance tasks, that are supporting two systems with thousands of named users."

The newest software solution from realtime, bioPortal, extends the security of bioLock to systems outside of SAP, such as databases like Oracle, DB2 UDB, and SQL Server, operating systems, and other applications. bioPortal combines the simplicity and security of biometric access control with the speed and convenience of “single sign-on” capability. With bioPortal, realtime has extended the concept of eliminating insecure passwords, beyond the realm of any existing IT security.

Summary

SAP consulting services continue to be a strong focus for realtime, and the foundation of their success. The average realtime SAP consultant has over 8 years experience. With headquarters in Tampa, Florida, an active staff, and a growing influence in North America, expect to hear a lot more about realtime North America in the future, as security continues to grow in importance for American corporations and government entities.

realtime’s expertise

Comprehensive, full-service solutions are realtime’s specialty. Products and services from realtime encompass the following:

- Consulting for SAP and E-Business
- Management Consulting
- Software for Industry and Security
- Application Service Providing
- Customer Support Center with Help Desk and Direct Service Line

realtime works with regional and proven cooperation partners in the area of hardware component maintenance and service.

For more information visit:
www.realtimeonorthamerica.com
Within the Trust

Wave Systems’ EMBASSY® Trust Suite Portfolio Enables Secure Business Computing

PC platform security has evolved into one of the most important issues facing today’s business computing marketplace. This may be due to such reasons as the rapid growth of wireless computing, the accessibility of corporate networks provided to the mobile professional or telecommuter, and the possible security holes that may exist in mainstream operating systems and applications. To address these issues, the industry is rapidly moving toward hardware-based Trusted Computing.

What is Trusted Computing?

An important demonstration of the momentum towards hardware-based Trusted Computing is the recent formation of the Trusted Computing Group (TCG), an industry organization dedicated to embedding trust and security more broadly into computing platforms and devices. The TCG has defined a semiconductor device known as the Trusted Platform Module (TPM) to serve as a “root of trust” for protected activities on enabled platforms. TPMs provide the trusted hardware resources used by Wave Systems’ services to extend trusted functions within a PC.

Through acceleration of the design, use, management and adoption of trusted systems for a variety of computing platforms, the TCG is helping the business computer users realize increased security through open standards. Earlier this year, Wave was among the initial industry leaders, along with Infineon Technologies, in instigating the TCG to develop, define, and promote hardware-enabled Trusted Computing and security technologies, including related hardware building blocks and software interfaces, across multiple platforms, peripherals and devices. Wave recently announced that Wave’s EMBASSY Trust Suite portfolio had been enabled on the Infineon Technologies TPM to make a secure computing platform, complete with an out-of-the-box suite of secure and trusted services and available to personal computer manufacturers.

Wave applications and services on the Trusted Platforms make a secure, high-value, services-rich computing platform available to businesses and personal computer manufacturers. And these capabilities are of course compliant with the recently announced TCG specifications.

EMBASSY Trust Suite - Wave Systems’ Client and Server Solutions

Wave Systems has identified the need for an introductory set of services on the business desktop and mobile platforms, in order to accelerate the user value of the trustworthy computing initiative. The company has developed the EMBASSY Trust Suite as a set of secure services that introduce the user to value-added applications in a manner that is intuitive and simple.

The current portfolio includes:

Document Manager Vault – The vault capabilities include; document encryption, decryption and client-side storage for important corporate documents. Documents are securely stored and easily accessible to the authorized user. The vault also allows multi-user functionality for an optional shared vault. The easy-to-use vault, utilizing Microsoft Office® integration, protects against unauthorized access from network snoopers and hackers (see Figure 1).

Private Information Manager (PIM) – The PIM uses the TPM to securely and efficiently store user information, such as user names, passwords and other personal information. The PIM intelligently retrieves login information for simplified Web login and automatic form-fill capabilities. The PIM’s data is securely stored using the TPM security features and can be moved securely from machine to machine (see Figure 2).

Smart Signature – This digital signature and document storage capability
includes signing keys generated by the TPM. Smart Signature is an Adobe Acrobat plug-in solution that is ideal for contracts or any other customized document or form that requires a signature. Included is a platform registration capability for storing and recovering Trusted Platform registration information and simplified back up and restore capabilities for the user or IT manager (see Figure 3).

Attestation Credential Manager –
The ACM provides capabilities for any application, to ensure that it is transacting with a Trusted Platform. It issues TPM identity credentials and certified credentials to provide attestation to a third party that a platform is trusted, and revocation checking ensures that the credentials are valid. This is a critical service for managing Trusted Platforms.

Key Transfer Manager –
the Key Transfer Manager is a web-based migration capability for archival of TPM keys and certificates, and utilizes tools to enforce business data management and access control policies. It provides IT administrators with the tools to service users in case of a TPM or platform malfunction, or to update to a new platform and is considered to be a logical and uncomplicated method for a business to manage its TPM-secured intellectual property assets.

Summary

Wave has leveraged its many years of research and development in security applications and trust infrastructures to develop this growing portfolio of embedded security solutions for the professional user. By adhering to a standards based approach to Trusted Computing, Wave Systems can assist its customers with evolutionary growth relying on broadly supported industry initiatives. Wave Systems has the products and services to enable an ease of use model for deployment, user experience and management of Trusted Computing platforms. This philosophy will allow the business users to leverage their training and knowledge to not only be productive, but also secure, as they embark on the digital commerce revolution which merely awaits the availability of Trusted Computing platforms.

Wave Systems Broad Experience in Embedded Security Solutions

A leader in delivering trusted computing applications, services and infrastructures across multiple trusted platforms, Wave brings years of experience in solving challenges in the trusted computing market. Prior to the formation of the Trusted Computing Group, and the emergence of the original TCPA embedded security specification, Wave developed and deployed its pioneering EMBASSY® Trust System in support of trusted computing. Largely targeted to next-generation smart card reader applications for government, military and financial services markets, the EMBASSY Trust System deploys and manages secure applications and services in a trusted environment. The EMBASSY Trust System provides secure hidden application execution capability, application lifecycle management and secure time based services. Today, with the emergence of the TCG-driven market opportunity, Wave is primarily focused on working with its partners in the PC ecosystem to deliver the EMBASSY® Trust Suite of applications and services. The Trusted Platform Module specified by TCG provides the trusted resources used by the Wave desktop and server services to bring these trusted functions to a PC computing platform. Wave applications and services for TCG-compliant platforms make a secure, high-value, services-rich computing platform available to enterprises and personal computer manufacturers.

For more information visit:
www.wave.com
WLAN – hot spot or damp squib?

A quick straw poll. How many of you know what a WiFi Hot Spot is? Quite a few of you I should imagine. But for those of you that didn’t – it is a public area, such as a hotel lobby or railway station, that is covered by a wireless access point, typically set up so that people can conveniently connect to the internet without cables.

To make you feel better, I should add that those of you who didn’t know are in very good company. A recent poll of around one thousand home PC users found that seven out of ten people had absolutely no idea as to the meaning of the phrase. According to the Mori poll, some believed that it was a type of ‘hot tub’ or a sun bed, while others thought it was a microwave meal. Of the ‘single’ people surveyed, a staggering one in ten believed that it was a nightclub. Most amusing were the people that thought it was an expression to use when they were in trouble with their wife.

This level of ignorance, while understandable, will no doubt change soon. Latest statistics suggest there are well over 4,000 hot spots in Europe, with this number growing fast. Still, one can only imagine what the public’s response might have been if the pollsters had stopped talking about WiFi and started talking instead about public wireless LAN (PWLAN) or 802.11b – which is the standard that most of these hot spots are based around.

I would be first to put my hand up and admit that I have hazy recollection as to the meaning of the standards surrounding the WLAN market. For those of you unawares, let me tell you there is a whole alphabet of 802.11 standards out there. They start at 802.11a and go all the way up to 802.11k, before skipping 802.11m – 802.11n is still some years away. The exact meaning of all these standards will have to be saved for another day. Some are mind-numblingly tedious, while others are actually worth a read.

One that I will venture to mention is 802.11i. But first I want to bring to your attention the results of another survey performed in the UK, which suggests that more than half of companies with a turnover of more than £50 million, have no plans to implement WLANs.

The survey was conducted by market research group Vanson Bourne on behalf of Cable & Wireless’ network infrastructure services subsidiary Allnet. To date, the survey says, just 7% of businesses in Britain have rolled out WLANs in any meaningful way, while 21% have pilot schemes in place and 16% have plans to implement such technology in the future.

WLANs can give freedom to workers and increase productivity, so why is it that big business seemingly remains to be convinced? According to the survey, 35% had issues with the perception of poor security offered by WLAN technology and 32% said they couldn’t afford it.

This finding comes as little surprise. The excellent article looking into the phenomenon of WarDriving earlier in this magazine explains very well the reasons why network security managers may be less than happy with the security features offered by current WLAN technology. It is still possible for hackers to stroll through a city or roam a building with laptops, a wireless network adapter and sniffing software in order to discover open or unsecured WLAN access points. With a little effort and a reasonable amount of traffic on the network, it is even possible to break the standard Wireless Equivalent Privacy (WEP) protocol within a few hours – and get access to a company’s sensitive data.

The soon to be released 802.11i standard could put an end to all of this and give back the WLAN industry some badly needed credibility in the security stakes. It eliminates some of the well documented security flaws that allow WarDrivers to ply their malicious trade. At that point perhaps those turned off by the problem of security may reconsider and provide fresh impetus in the corporate WLAN market, turning it once more into a hot spot sector, rather than a bit of a ‘damp squib’.

As a side note, is any of this sounding familiar to readers from other industries – say the biometrics sector? Let’s see: users unaware of the technology; security PR problems (note the ‘gummy finger’ debacle); a plethora of confusing standards; and users not being able to afford the technology. For sure, these are all current headaches.

The hottest topic in biometrics at present is the introduction of biometric passports (see page 21). I tried explaining to an elderly relative recently that she may soon have to visit an enrolment center, pay an inflated fee for her passport and have her biometric (what?) taken – face present. Let’s just say that from the look on her face, I foresee big user acceptance problems ahead. Not insurmountable, but from this narrow viewpoint, it is a shame that the UK government has now said that ‘spin’ will no longer be a part of its politics. Interesting times ahead.

Mark Lockie