

the gemalto

# Review

OCTOBER 2006

## SECURED IDENTITIES

PAGE 12

YOUR IDENTITY DIFFERS DEPENDING ON WHO YOU ARE ADDRESSING. SO HOW CAN WE KNOW WHO YOU REALLY ARE?

**E-commerce** opens up opportunities – and risks **PAGE 04** Convergence sparks an **m-transformation** **PAGE 06**  
How to hedge against **virtual thieves?** **PAGE 20** Systems integrator reveals his **secure solutions** **PAGE 22**

+ The new name in the digital security market is already a world leader. **PAGE 10**

**gemalto**  
security to be free

# What do you want to do?

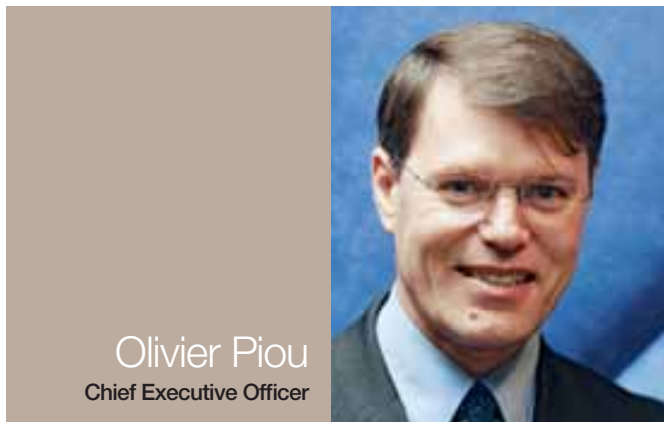
Check your email, shop on-line, phone a friend... I could go on! But chances are, whatever you do, you'll do something digital.

It would be difficult not to. With 2005 seeing 1 billion Internet users, over 2 billion mobile phone subscribers and sales of over 3 billion banking cards, there's a good 50/50 likelihood you're at least one of those statistics, communicating or transacting using digital technology.

Its extraordinary growth is affecting individuals, businesses and governments all over the world. And with the simultaneous spread of global communication systems, personal computers and the Internet, it is enabling virtually any form of data and media to be shared, used and enjoyed in an increasing number of ways.

These developments are clearly changing our lives in revolutionary ways. Some things are much faster, more enjoyable and more convenient. We can be more informed, more efficient, and more entertained; we certainly have more options, and we can have them instantly.

But all this freedom inevitably raises many issues, of which the most fundamental are to do with identity and security. If I am trading on the Internet, completing my tax form or delivering TV to a mobile phone, how can I know that



Olivier Piou  
Chief Executive Officer

“All this freedom inevitably raises many issues. The most fundamental are to do with identity and security.”

the person on the other end of the line is who they say they are? How can they confirm their right to receive my money, data or services? How can I be sure no-one is siphoning off my details as I send them, so they can defraud me? How can I even confirm that I am me?

These issues are perceived to be so significant that they are preventing us from getting the full benefit of digital technology. To do that, we clearly need to have adequate measures in place to preserve personal identity, create trust and protect privacy. In other words, we need security in order to be free.

It is to answer these issues and respond to the opportunities of the digital age, that we created Gemalto. Built upon the foundations of the two leading players in the smart card sector, Axalto and Gemplus, Gemalto has unmatched experience in the innovation and fabrication of secure personal identifiers.

We are now taking our combined experience into this wider, rapidly expanding market of digital security. Benefiting from the opportunities provided by evolving and converging technologies we aim to protect, facilitate and enrich people's interactions with the networked world. Though our software platforms are taking an increasing number of forms they have the same inherent qualities of security, convenience, and personalization.

As Gemalto's CEO, I am delighted to introduce our new magazine to you since it takes a look at the global context of this visionary move, and examines some of the many ways in which these vast issues and technologies touch our everyday lives.

I hope it makes for interesting reading.

**Editorial Office** Kynämies Oy, Köydenpunojankatu 2aD, 00180 Helsinki, Finland, tel. +358 9 1566 8510 | **Editor-in-Chief** Paul Beverly | **Changes of address** magazine@gemalto.com | **Publisher** Gemalto N.V., 6 rue de la Verrerie, 92197 Meudon Cedex, France, www.gemalto.com, tel.+33 (0)1 55 01 50 00 | **Printing** Frenckell Printing Works Ltd. Niittyrinne 4, 02270 Espoo, Finland | **Cover photo** Getty Images / Altrendo | Z4018561

**gemalto**  
security to be free

“We have an awful lot of identities,” says  
PAGE 12 Joel Shaw.

|                 |    |  |
|-----------------|----|--|
| BUSINESS TOPICS | 04 | What is going on in the industry?          |
| ABOUT GEMALTO   | 10 | Brand-new world leader.                    |
| COVER STORY     | 12 | Who are we?                                |
| FUTURE          | 20 | How to fight against virtual thieves?      |
| TECH CASE       | 22 | What do secure systems consist of?         |
| END USER        | 26 | A credit card can also feel and look good. |



“The best security systems probably rely on both software and hardware.”  
PAGE 22

# Increasing trust Securing e-Commerce

The advent of e-Commerce – the buying, selling, marketing, and servicing of products or services over computer networks – has opened up huge business opportunities, and plenty of risks too. Top of the list is on-line identity theft. According to **Kerry Loftus**, Director of Product Management for VeriSign's authentication services, hackers are becoming more sophisticated.

"Phishing and pharming are the two largest drivers of on-line identity theft," he says.

In fact, it looks as if phishing is even catching up with viruses and malware as major issues for the Internet. In 2004, one message in a thousand was a phishing attempt – in 2005, one in three hundred.

"The industry has taken a number of steps to address the phishing problem, and there are some tools on the way that will help dramatically in the battle against it," says

**Tim Callan**, group product marketing manager for VeriSign. Together with other industry players, VeriSign is currently working to develop an industry standard for High Validation SSL certificates. When used with Microsoft's new IE7 browser, these will more clearly identify websites that have passed the highest level of the authentication process.

## ENHANCING PROTECTION IN ASIA.

It's in the light of these issues that the USA's Federal Financial Institutions Examination Council (FFIEC) has published guidelines stating that user names and passwords are no longer sufficient for high-risk transactions. By applying two-factor or multi-factor authentication, banks can lessen their vulnerability to fraudulent transactions.

In Singapore, in response to an advisory issued by the Monetary Authority of Singapore (MAS), banks are gearing up to provide two-factor authentication at login for all Internet banking systems by December 2006. ABN AMRO, which opted for this type of system when it launched its Internet banking service two years ago, uses a hardware-based, dynamic security generator as the second

For the IT industry e-Commerce includes electronic business applications as well as electronic data interchange (EDI) and automated data-collection systems.



authentication factor because of its wider acceptance.

Multi-factor authentication includes a fraud detection service that monitors each user's typical online behaviour and can prompt for further authentication. Two-factor authentication helps to ensure that people are who they say they are. To get the message across to users, ABN AMRO has assigned dedicated staff to demonstrate the use of the password-generation device to every client who signs up for its Internet banking service.

**Ross Wilson**, Managing Director for South Asia and India at RSA Security, said in an article published by ZDNet Asia in May 2006 that banks also need to look beyond authentication. "With fraudsters exhausting the various avenues in North America and Europe, they are looking for 'greener pastures' within Asia. Local banks should definitely start looking into implementing a layered approach to safeguard their customers before online fraud becomes more prevalent here," he said. |

**PHISHING |** A form of criminal activity characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is typically carried out using email or an instant message.

**PHARMING |** The exploitation of a vulnerability in DNS server software that allows a cracker to acquire the domain name for a site, and to redirect, for instance, that website's traffic to another website. DNS servers are the machines responsible for resolving internet names into their real addresses – the "signposts" of the internet.

**MALWARE |** software designed to infiltrate or damage a computer system, without the owner's consent. It is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. In law, malware is sometimes known as a computer contaminant.

# Achieving stability and durability by standardization

The buyer of identification products and technologies faces a choice: to use proprietary or standardized solutions.

Despite their apparent interest, proprietary solutions have certain drawbacks. A project may be more complex to design and implement and more expensive to source and maintain since it does not rely on existing standards whose mechanisms have already been defined. Users' mobility may also be limited due to the lack of interoperability of applications.

In general, these considerations are slowing down the deployment and adoption of e-ID schemes.

Governments and corporations alike are therefore tending to turn to standardized solutions. In particular, they want the twin guarantees of stability and durability. This is especially so when they realize that by using standardized technology they will not be reducing the options for tailoring the application to their particular needs.

They are also driven by the need for interoperability, for example in the context of increasing international travel and trade. Typically, a passport needs to be usable anywhere in the world, regardless of the system adopted by the home nation. Equally, interoperability is a must for companies conducting transactions with customers and suppliers who may be using quite different technologies.

**COMBINING TECHNOLOGY AND LEGISLATION.** It's therefore not surprising that standardization efforts are mainly driven by international bodies, such as the International Standard Organization (ISO) and International Civil Aviation

Organization (ICAO), though regional and national organizations also play a role.

In the case of an e-ID document, standardization covers many areas, from its logical data structure (which specifies the way in which it stores a wide range of information) to security mechanisms, certification evaluation and even test methods.

For e-passports, the ICAO has defined a common logical data structure and security mechanisms. It is also steering the work of several standardization groups within the ISO organization, including those in charge of biometrics and contactless technology.

In the case of common security mechanisms, the European smart card industry is working on a common framework for ID applications – IAS (Identification, Authentication, Signature). This framework allows for interoperability between ID applications and increases the level of security. IAS relies on existing standards and certifications (ISO 7816, ISO 14443, Common Criteria Protection Profile, E-Sign digital signature) and the work currently done on IAS is being pursued further by the standardization committees.

Yet in itself, the existence of a common technological standard does not necessarily mean it will be used. A legal framework also needs to exist. Take, for example, digital signatures in Europe. It is clear that the adoption of signatures did not start because of the standards, but rather due to the legislation recognizing their use and even making them mandatory in some countries.

This transversal approach brings together government and industry players to combine standards and laws for mutual benefit. The effect is to regulate industrial transactions and enhance both the quality of products and the level of security. This is the best guarantee of success. |



“Governments and corporations are harmonizing standards for mutual benefit.”

# Telecom transfo

The convergence of the mobile and Internet worlds is good news for subscribers – and presents huge opportunities for operators.

One billion people are using the Internet these days – and 2 billion are using mobile phones. Those figures alone testify to the extraordinary advance of digital communication.

Imagine, then, the possibilities when those two worlds converge – when things that were once only communicable via the Internet become accessible on a mobile handset, and when mobile services can be accessed via a PC.

For many subscribers, that's already the reality. Those with the right device and a high-power SIM can browse the Internet and send emails, conduct financial and other transactions, watch TV, play music and video games, listen to the radio, take photographs, download and watch streaming video, and send their photos and videos to a personal computer.

But they are not necessarily doing this within a standard mobile environment. When it comes to new digital services, end-users now have a huge choice of content and providers that goes beyond a standard mobile subscription.

For example, many are choosing other technologies for their home communications such as VoIP or Instant Messaging that are not normally found within an operator's portfolio - just one sign of the complexities that lie beneath the surface of mobile convergence.

**END-USERS HAVE MASSIVE CHOICE.** The fact is that convergence can also mean complexity. The opportunities are there, but for users and operators alike it is not always obvious how to reach them.

As the options have become ever more rich and varied, they have also become significantly more complicated, and this is holding users back from enjoying the full benefits of the new mobile world.

With all these choices, they are finding that their handset menus can be tiresomely complex, slowing their access

to (or even knowledge of) particular services.

The use of content is also becoming more complex. With Megabits of content stored in several memories (handset, external slot, SIM) on different supports like removable memory cards, multimedia cards and memory sticks, content management is becoming cumbersome for end-users. Moreover, they have to contend with the fragmentation of the

content format, as well as DRM issues that hinder portability from one handset to another.

In addition, multimedia contacts are currently stored on the handset, preventing easy portability of the multimedia phonebook, and generating revenue losses for telecom operators.

As a result, end-users are clearly in need of a new generation of tools to help them manage their new mobile environment without having to worry about devices, space or time, and enable them to experience true convergence: a convergent phonebook, interoperable digital content and a set of common communications tools for the home, the office or elsewhere.

To get just that, they need a convenient digital solution capable of



# rmation

handling the size of the files involved; of enabling portability between different devices and platforms; and of delivering strong security so they feel confident that the personal information they are storing and transactions they are making cannot be breached.

**MOBILE OPERATORS FACING THE CHALLENGE.** But in this environment, it's not only end-users who are caught up in the swirl of change. The current positioning of mobile operators is also being challenged, particularly given the increasing involvement of big Internet brands offering new mobile services and changing market dynamics.

While operators have been focusing on their core mobile business, digital newcomers like Internet service providers

have been crossing the divide and entering the mobile space. Using new network capabilities, they are now addressing end-users directly to offer a mobile extension of their web services – which means they are directly targeting part of the operators' revenues.

So operators too are confronted with a wide range of issues. First of all, they are facing a fragmented segmentation of their user database. From teenagers developing communities via instant messaging or blogs on the WAP, to corporate users, operators need to adapt their offer to each market segment.

An additional threat is also coming from new technologies that are opening the handset environment and offering potential bypass of the mobile network. Free content can now be uploaded

directly from a PC to a handset using a USB cable, Bluetooth and Wi-Fi. Internet service providers are already providing free content through their sites accessible via the WAP, competing with operators' premium services and business models.

**THE POWERFUL ROLE OF MULTIMEDIA SIMS.** Thus in order not merely to cope with the new factors of the digital age, but to benefit from them, operators need solutions that provide three things: flexibility, so that they can deal with the myriad different problems of software and hardware interoperability; capacity, so that file size (in the era of photos, video, games etc) is no longer an issue; and security, so that they are confident that the services they are delivering are going to the right subscribers.

With exactly these attributes, and covering the full spectrum of telecommunication and multimedia services, the new generation of multimedia SIMs can empower their positioning in this evolving landscape. ➤



“Operators need solutions that provide flexibility, capacity and security.”

## SIM – key assets

- > It is the **operator's property**, a unique token expressing the relationship between operator and subscriber.
- > It ensures a **secured authentication** of subscribers on the operator's network.
- > It can be totally **personalized** to fit an operator's requirements.
- > It represents a **personal storage space** offered by operators to subscribers.
- > For end-users, it is seen as a **secured and portable environment**.

In the new generation of SIMs technical barriers such as memory and speed have been removed. This transforms the cards into a platform that allows operators to offer a full range of multimedia and telecommunications services beyond the traditional mobile world, and enables them to connect the SIM to the PC in order to access Internet services, bringing multimedia content and contacts onto the card. As a result, they can regain their relationship with their subscribers by offering a service that is both more rich and more user-friendly.

With this technology, operators can offer multimedia services through various channels, including mobile, web and broadband TV. At the same time, their subscribers can share multimedia content between devices and access new services from their PC or mobile phone. With a phonebook that is fully adapted

to Mobile/Internet convergence and new digital identities (e.g. VoIP number, IM nickname, Blog URL, etc.) they can also manage and synchronize their contacts via their PC and transfer their multimedia contacts from device to device.

The operator can also target new services and applications for different market segments, updating the user interface 'over the air' to suit different profiles or in response to user behavior.

Crucially, they have the freedom to do all this within a secured and convenient environment. Since the SIM offers a highly trusted means of secure authentication, operators are certain that whatever they are providing is going to the right people; and subscribers have the convenience of using one single identifier to access multiple services, safe in the knowledge that they are correctly paying for what they have requested.

**M-COMMERCE: SECURITY IS PARAMOUNT.** Advanced technology has also enabled mobile devices to be used for "m-commerce": buying and selling on the move. This means that consumers can nowadays conduct bank and stock market transactions, access accounts, and publicize and pay for products and services from mobile devices.

Tech-friendly Asians are especially keen on using mobile devices for banking. The Bank of Korea recently reported

that the number of mobile banking transactions in South Korea in 2005 rose to a daily average of 287,000, up 104.4 percent from 2004.

Although the m-commerce market is still relatively young, many commentators confirm this trend, seeing huge growth potential. Consultant firms IDC and Jupiter Media Metrix estimate that the m-commerce market in the United States alone will grow to a staggering \$ 58.7 billion in 2007.

M-commerce functions by the interaction of once discreet sectors: banking, telecommunications and the Internet. This has created a limitless number of wide-ranging opportunities, but has also created a number of issues around security, which is clearly vital to the long-term success of m-commerce. In a mobile environment where money is exchanged, data is communicated, services are delivered and identity is demanded, it is strong security that brings trust and confidence to an otherwise vulnerable situation.

With rapid advances in this domain, enhanced security mechanisms are already on the market. SIM cards equipped with powerful encryption and digital signature capabilities can enable highly secure transactions. This is a key factor behind the significant increase of mobile banking transactions worldwide. |

\*According to The Korea Times, February 2006



## Mobile-TV: little screen, big business!

**MOBILE-TV** (m-TV) is captivating end-users worldwide – and represents a potentially valuable business model for mobile operators.

But if they want to take advantage of this new wave and act as the next generation of pay-TV players, operators will need to use a technology delivering a high level of security.

In that respect they have two main options. The first is a solution based on the UMTS network, offering a point-to-point technology but consuming high bandwidth capacity, thus limiting the contents and the number of simultaneous channels.

The second is broadcast using the USIM Conditional Access

Solution (CAS), offering operators a wider range of possibilities. This fits the standardized ETSI Open Security Framework (OSF).

Many broadcasters already use a security scheme based on smart card technology for Pay-TV, while operators already deploy and control the USIM. Thus this technology is playing a key role in the m-TV boom, enabling operators and broadcasters alike to safely enter the m-TV world. It ensures secure, convenient access to operators' broadcast programs, and enables them to position themselves distinctively by also offering interactive multimedia services like content downloading and voting.

# No hassle with One-Time Passwords

The One-Time Password is both practical and easy to use. And what is more, no big investments in infrastructure are needed. That makes it ideal for small and medium-sized companies.

The oldest and simplest form of authentication is a password. However, in today's world it is no longer considered safe enough. Hidden costs such as help desk support are often underestimated and present another significant disadvantage.

For more reliability, at least two forms of authentication are needed, such as a smart card in combination with a PIN code. Using two methods or more is referred to as "strong authentication". There are basically three different forms of authentication that can be combined:

something you have, such as a smart card or a hardware device; something you know (a password); and something you are (fingerprints or other biometrics).

**SIZE MATTERS.** The two most commonly used forms of strong authentication are One-Time Password (OTP) and Public Key Infrastructure (PKI). OTP is a two-factor method while PKI relies on mutual factors.

While it is getting easier to implement PKI, considerable investment in new tools and infrastructure is still needed. PKI is therefore more suitable for larger enterprises that require a more comprehensive form of authentication that secures users and the information they exchange over the network.

For small and medium-sized enterprises, OTP authentication can provide a solid and secure starting point for a stronger form of authentication than using passwords. For small companies, who already have company badges to allow access to buildings, OTP is ideal. Subsequently, they can use smart cards or smart card based devices and tokens for

generating OTPs and then use the same device to hold a PKI credential once the enterprise is ready to do so.

**PRACTICAL AND EASY.** OTPs are usually generated by portable hardware devices called OTP Tokens. Apart from those, no other investments in either infrastructure or hardware are necessary. In addition, OTP is simple to integrate and to use.

With OTP a new password is generated each time secure access to the network is required. This means that the password is only used once, and that thereafter it is no longer accepted by the authentication server. This makes OTP the most efficient way to address replay attacks.

OTP can also be used by the general public. Some banks already have it in use for their customers. Rather than a password, customers use the OTP Token to generate a password each time they go online. The OTP Token can also be combined with the customer's bank chip card.

Gemalto's authentication solutions supports both OTP and PKI. |

# gemalto

security to be free

Gemalto is a new name in digital security, but still has decades of experience in the field.

Gemalto is a world leader in digital security. Formed in June 2006 by the combination of Axalto and Gemplus, we unite their vision, capability and innovative powers for the benefit of our clients.

In an increasingly connected society we make personal digital interactions secure and easy, enabling governments, organizations and businesses to offer trusted, convenient solutions to the billions of people who use digital networks for communications and transactions, setting them free to make the most of the digital world.



## Devices, platforms and services

Gemalto provides devices, services and ready to use solutions based on secure software platforms for applications for the digital world:



- > Personalization services including data management, file treatment, post-issuance and packaging services
- > Operated services
- > Consultation, integration, project management and maintenance, training and support services

### Secure platforms

- > portable, secure and personalized forms of software embedded in various personal devices
- > microprocessor cards: smart cards such as wireless SIM cards, payment cards, identity cards etc.
- > e-passports, healthcare and e-ID cards
- > a wide range of pre-paid cards for public telephony
- > tokens, USB dongles, readers and chipsets

- > Point-of-sale: a complete range of terminals, dedicated software tools, management systems and services

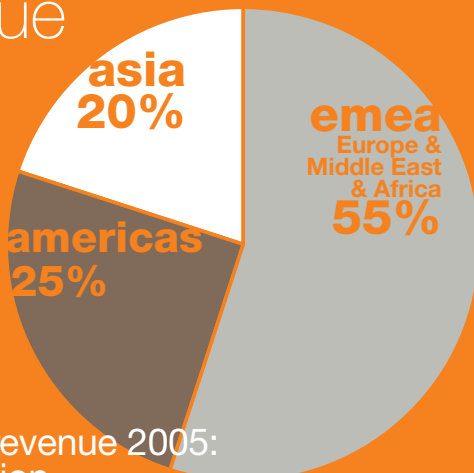
### We also provide

- > Associated software, middleware, and server-based solutions

Whatever their form, Gemalto's innovative solutions are **secure, convenient and personalized.**

## Our assets at your service

Revenue



Pro-forma revenue 2005: US\$ 2.2 billion

Personnel

11,000 employees

85 nationalities based in over 40 countries on every continent

# Our values

We put **their needs at the center** of all we do, develop partnerships and **exceed their expectations**.

our customers

our people

We value their diversity, encourage teamwork and conduct ourselves with integrity.

We continually develop valuable new ideas and **creative approaches** to business and technology challenges.

our innovation

## Key markets

### Telecommunications

- > mobile and fixed network operators

### Banking and Retail

- > financial institutions, card issuers and retailers (loyalty)

### Enterprise

- > businesses and organizations (physical and logical access, e-purse, digital security etc.)

### Internet Content Providers

- > Internet service and content providers, on-line retailers and pay TV

### Public Sector and Transport

- > governments (passports, visas and ID cards; health care solutions; driving licenses etc.) and mass transit authorities (passes and ticketing)



## Service and supply

- > A global vision matched by a regional structure
- > Harmonized and flexible processes across all 24 production sites and 31 personalization centers
- > Uncompromised secure assembly and personalization facilities
- > World class standards and practices: ISO9001, ISO14001, OSHA18000, MasterCard CQM, 6σ
- > World-class supply chain logistics for rapid reactivity, short lead-time and high security

## Innovation

Our commitment to our clients is reflected in our commitment to R&D. They demand an ever-wider range of innovative, high-quality solutions, so we invest to meet their evolving needs.

Gemalto has by far the largest R&D team in the industry, employing 1500

R&D engineers, including internationally renowned researchers in security and cryptography.

With thousands of patents and patent applications, and more every year, we have a renowned, long-term track record of innovation.



## Locations

- 24 production sites
- 31 personalization centers
- 10 R&D centers
- 117 sales and marketing offices



# Who are

TEXT Rick McArthur PHOTOS Mika Ranta

QUESTIONS OF IDENTITY  
HAVE ALWAYS BEEN AMONG  
THE MOST FUNDAMENTAL WE  
FACE. WHILE IDENTIFICATION  
TECHNOLOGIES ARE  
CONTINUALLY EVOLVING, IT IS  
WORTH RE-EXAMINING WHAT  
WE ACTUALLY MEAN, OR THINK  
WE MEAN, BY IDENTITY. >



A person is walking from left to right across a highly reflective, blue-tinted floor. The person is wearing dark trousers and dark shoes. A black suitcase is being pulled on the left side of the frame. The floor is made of large, light-colored tiles that reflect the ambient light, creating a shimmering effect. The overall color palette is dominated by various shades of blue, from deep navy to bright cyan.

we?

“We’re in a time when  
the management of  
identity is much  
more important to  
the government and  
the public.”

**JOEL SHAW**, Chief Strategy Officer of CryptoMetrics, tells how many identities he thinks we have. “An awful lot, probably more than we need. I guess, unfortunately, they all differ depending on either who is establishing our identity or who we are addressing. We have a wide range of documents, every one is different, and everyone seems to have their own database, so it would be nice if we had a single identity.”

Can this problem be solved? “I think that the events of the past couple of years, the change in the modus operandi of terrorism to suicide terrorism and non-conventional terrorism has raised the whole spectre of how important it is to be able to confirm identity. Naturally, identity theft is just below that “peak”



## No caller ID

**Gilles Lisimaque** has given some thought to when the ‘problem’ of identity began.

“I think it started with the telephone system, because that was the first time we were able to get into the private homes of people without knowing who really was on the phone at the other end. We relied first on the system that was connecting us, then we relied on the voice being known, and now we have the caller identity information given to us by the system. Right now in the US, we feel very nervous when ‘No caller ID’ shows up. We simply have no idea who is calling – and we like to know who we are talking to because we’re in a world of almost completely anonymous, unknown relationships.”

level but you still have, for example, illegal immigration, and trafficking in human beings. All of these begin to have an impact and accentuate how important it is to have identity details that can be confirmed accurately and efficiently.”

In Joel’s opinion, governments are beginning to realise the importance of identity confirmation and are moving towards something of a more universal and more effective approach over the next 5–10 years. “When you look at the events of the past few years, there’s probably no panacea. But the one thing that stands out is that if we’re able to better identify people, we might be able to prevent some of these things.”

Secure forms of electronic identity would of course have significant beneficial effects on international travel, speeding up the processes involved at border controls, for example. Many public services are also becoming easier to access for individuals who have identity tokens in electronic form.

**Who are you talking to?** Gilles Lisimaque, a leading US expert on smart cards and their applications, takes a different approach, sharing an experience he had in the southern hemisphere. “I was on a working trip in Australia, and I visited a tribe called the Tiwi. When I asked one of those guys down there his name, he paused for a second and said ‘Well I have different names depending on who I talk to’. And in that tribe, they have just that – a name for use with their parents, a name for use with their family, a name for the neighbours, a name for the tribe and a name for other tribes. I’m mentioning this because it struck me then so clearly that their identity is something they reveal depending on who they are talking to. And that’s also very interesting because we’ve lost the whole notion that who we are depends on who we are talking to – and when we talk about establishing or confirming an identity, it really does depend on the role we are playing.”

We shouldn’t think of identity as something that is cast in stone, an absolute, says Gilles. “An identity is something based on your past and on the relationship you have with the person you are talking to. So if we think about defining our identity, as buyers we have an identity for people we don’t know; with neighbours we have an identity with people we know better; with families we have an identity which is different again; and when we cross borders we have yet another identity. In actual fact,

## Glossary

**IDENTITY** | The individual characteristics by which a thing or person is recognized or known.

**IDENTIFICATION** | A means of identifying a person or thing.

**BIOMETRIC IDENTIFICATION** | The automatic identification of living individuals by using their physiological and behavioral characteristics.

**AUTHENTICATION** | The process of verifying that something is genuine.

**BIOMETRIC AUTHENTICATION** | Any method of verifying the identity of a person by measuring their physical features.


our identity is something related to what you do at a given point in time, based on past transactions you have had with these same people.”

**What is a positive form of identification?** According to Joel Shaw, there have in the past been two main methods of confirming that your identity details really belong to you: accepting the document as valid simply because you’re holding it, or checking the photograph to see if it looks like you. “With the introduction of biometric travel documents, we show just how easily a positive identification can be carried out. In the future, therefore, even in cases where I had managed to obtain your data, a positive check of your identity details will expose me as not being the rightful holder. This will raise the protection level, making those details of no value to a thief because if a positive check is carried out they will be caught.”

Does he think this will come to North America? “There is clearly a movement towards it. I’m not sure whether it will manifest itself in the form of a national ID card. But with the US government’s specification of ID documents for specific groups of workers, for example, and e-passports, we’re moving towards a time when an identity, or the management of that identity, is much more important to the government and the general public.”

### Management is what matters.

But can a name and a number actually be attached to somebody, a person, in a fixed manner? Gilles Lisimaque challenges that assertion. “The name and number that you are talking about >



“With the introduction of biometric travel documents, we show how easily a positive identification can be carried out.”

**IDENTITY IS NOT JUST  
PROTECTING DATA**

According to Joel Shaw, we have to embrace the fact that we would have much better ways of protecting ourselves against identity theft and terrorists if we have more positive ways of identifying ourselves.

“The data becomes far less important. The fact is that if you do a check and confirm that I really am Joel Shaw, then that’s the most important thing, it’s not the data. I think our historical focus, given what was available to us, was: to protect the data.”



Mini  
Miss  
Lift

2  
P

is what is used by identity thieves, but the name and the number always relate to the entity which has vouched for that number. Your passport number has been issued by that country. Your social security number has been issued by a country, and so forth. So that number which is attached to you is not really an identity, it's more something which is both an identity and a number that somebody is managing. And we usually forget that notion. And when the number is used for something else than what it was designed for, then identity problems arise."

Commenting on the situation in the USA as an example, he says that social security numbers, created by the US government to distribute benefits, have been used as identification numbers to track people's financial behaviour. "That misuse of the number created the problem. That's why I love the story about the Tiwi – if you have an identity which is related to one given role, one relationship, well the numbers do not have the same value and so are harder to misuse for another function."

**Creating identity at birth.** France has a system that uses social security numbers, says Gilles Lisimaque. "In France, you have to have identity papers with you all the time when you are outside on the street. In the US it's the other way around. And I have found that identity theft generally happens in societies where they do not want to prove their identities. The fact that people in the US use their driving licences as identity documents is the source of most of the problems." Driving licences can

## “Do identities need to be protected, or are they something which should be so strong that this is not necessary?”

be obtained using documents which can be weak, like birth certificates, and from there you can build an identity on very false assumptions. "When you have societies like France or Finland, where the state creates an identity at birth and then maintains it, it's much more difficult for it to be misused."

Can we then protect our identities – do they need to be protected, or are they something which should be so strong that this isn't necessary?

Joel Shaw: "I believe that we all have to stop and think about it. The traditional approach to identity confirmation is to ask for information; in some cases more and more information, until the level of knowledge suggests I am that person. In the traditional sense, the only way to do this is to use a photograph when it's available. What's interesting here is that we focus on global interoperability with these new machine-assisted approaches we're taking." In Joel's opinion, the method of achieving global interoperability using traditional documents is simply via the photo they carry. "That's the only way I can hand

a document to a passive system, one in which a human being is the validating component, and quickly and effectively confirm my identity."

**A human interface.** How about the cards or passports themselves? Is there >



The height or the color of eyes of a traveller can be regarded as biometric identification.

## What is biometric identification?

A biometric identifier is a measurable physical or biological feature which serves to single out an individual. Biometric identification may sound new but it is in fact a long-established way of identifying a person. The way in which a border official formerly used a passport to check the height or the color of eyes or hair of a traveller can indeed be regarded as an instance of biometric identification.

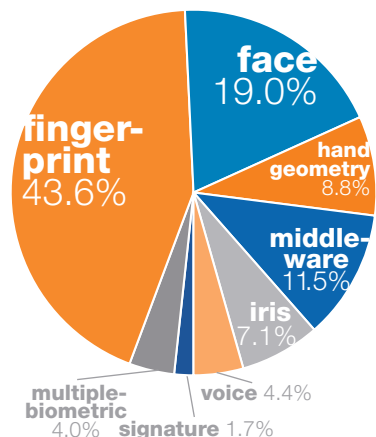
Biometric identification, as a method, is a technology in which a person's physical or biological characteristics are used for identification purposes. Among the most common of these are fingerprints, facial pattern,

voice, the iris of the eye, hand shape, signature, keystroke, and palm recognition. A person's DNA, ear shape, smell, blood vessel pattern, finger geometry, tears or gait may also serve as biometric identifiers.

The current state-of-the-art product in biometric identification is the biometric passport. Its built-in microchip can be used to store various biometric identifiers.

Biometric identification finds an application in electronic services, access control, logging on to computers and computer systems, ATMs and payment terminals, electronic commerce and services, plus crime investigation and travel.

**Biometric market**  
by technology, 2006





The application of biometric identification is being pioneered by public authorities in the introduction of biometric passports, or e-Passports.



## Who?

**Joel F. Shaw** is the Chief Strategy Officer of CryptoMetrics. An internationally acclaimed expert in the field of machine-readable travel documents and border management systems, Mr. Shaw has spent more than 18 years conceiving, designing and developing border clearance, airport security and document-reading systems. Mr. Shaw is a co-author of a patent dealing with securing of travel documents.

Before the acquisition by CryptoMetrics, Mr. Shaw was the founder of BioDentify. Previous to founding BioDentify, he served as Executive Vice President of AIT.

Mr. Shaw has worked closely with the Canadian Passport Office, the U.S. Department of State and the U.S. Immigration and Naturalization Service. He is also the Chairman of the International Standards Organization (ISO) Working Group.

**Gilles M. Lisimaque** is one of the leading US experts on smart cards and application of smart cards, working on various US government projects as technical advisor and smart card standard expert. Prior to joining IDTP Mr. Lisimaque worked at Gemplus, a company he founded with four other co-founders.

Prior to joining the Gemplus team, Mr. Lisimaque was technical marketing director in SGS-Thomson's research and development group. Additionally, he was MIS manager of the SGS-Thomson MOS facility called Eurotechnique, a joint venture between Saint-Gobain and National Semiconductor. Mr. Lisimaque holds multiple patents on smart card security and smart card OS design and has high level seats with numerous smart card and security forums and associations.

any way we'll move away from the need to have an item which can of course be lost mislaid or stolen?

"I guess technocrats would say 'Absolutely – we don't need any of this,'" says Joel Shaw. "But I think that these documents and the need to present an identity and confirm identity comes back down to that terminology again – global interoperability. And so we come back to a system that is largely human based, where someone looks at something and then decides to take a specific action. Each of us has to have a mechanism to interface with that 'system'. And that's where a high-security document with a photograph on it allows the interchange to take place. And to me, in an academic sense, that's what the new biometric passport has clearly demonstrated to those of us who are deeply involved in it. We recognised that this was a system, that we had to develop something that works across all aspects of the system, even those that are not supported by machines. As with many systems, you have this one frequently-used component – the human being. We have to have a card or a passport that works when only the human being is present."

**Liability for initial disclosure.** How about governments holding onto the information once they have it?

Gilles Lisimaque: "There's a major difference between the US and European law as regards private information. In Europe, whoever is the custodian of a piece of information that can point to me is liable for that information in terms of misuse of the initial disclosure. It's a liability which is part of the law. In the US, such liability does not exist unless I enforce it. That's the 'opt-in' and 'opt-out' notion. And this changes your view of corporations completely. Because in the USA they are abusing this information – they are selling it, they are making money out of it, that's part of what they do. The government, on the other hand, is pretty well controlled and some appropriate laws exist – disclosures

do happen, but they are much less consequential than those resulting from the activity of commercial companies."

Commenting on the case of a company about to go bankrupt which changed its policy regarding private information and tried to sell the information it possessed in order to make some money, Gilles says "I think that was outrageous and should have been banned by law."

And Lisimaque has a final point to make concerning identity theft. "The interesting thing is that the extent of identity theft is over-estimated. In most cases, the term is used for people that misuse a card number, and in my opinion that's not identity theft, it's simply misuse of an account number. The banking system corrects it and I don't regard that as much of a problem. Real identity theft is something much smaller in scale than most people believe, but much more complex and harmful. What are really serious are cases like the one where after driving up to your summer house, you find people living there because it has been sold in your name. That's what I call identity theft. Misuse of the term just doesn't help." |

“There’s a major difference between the US and European law as regards private information.”



## Higher security – stronger identification

The market demand for high security products is increasing, whether for use as a means of identification in face-to-face dealings or for secure authentication in online transactions. The characteristics of a secure product include resistance to counterfeiting, easily verifiable authenticity, and reliability as a means of identification.

The application of biometric identification is currently being pioneered by public authorities around the world in the introduction of biometric passports, or e-Passports.

The growing interest in e-Passports is a

direct consequence of the US Government's decision to require, from October 2006, biometric passports from those countries whose citizens have previously been able to travel to the USA on a visa waiver. Another important reason is the EU legislation that will also require EU member states to introduce biometric passports from August 2006. Furthermore, the International Civil Aviation Organisation (ICAO) has created specifications for biometric passports, and this also plays its part in promoting their introduction in different countries.

As electronic identification becomes more common, the demand for more secure and difficult-to-forge e-ID cards will grow also. Thus, a microchip including biometric identifiers and several visual security features will be incorporated into the ID cards of more and more countries.

These more secure biometric passports and e-ID cards represent the response of authorities to the greatly increased security pressures caused by the growth of travel, the threat of terrorism and illegal immigration.

# Virtual thief

— practical solutions

Tony Neate  
E-Crime Liaison Officer,  
Serious Organized  
Crime Agency



“Virtually organized gangs meet and coordinate their activities on the Internet.”

The Internet has become an Aladdin’s cave for career criminals to plunder. Smart thinking can stop would-be thieves before it’s too late.

TEXT Anna Mård  
PHOTOS Petteri Kokkonen

## THE VIRUS-SPREADING

hackers of yesteryear are no longer the news-makers. Internet-based criminal activity is more organized and professional than ever before. The new generation of thieves plunders for financial gain and not just for the fun of spreading mayhem. But solutions are available to stop would-be criminals in their tracks before financial loss is suffered.

According to **Tony Neate**, E-Crime Liaison Officer of the Serious Organized Crime Agency in the United Kingdom, the criminal

faction knows where money is to be found and what kind of information is needed to acquire it.

“New-age organized crime is typically the domain of highly educated and relatively young people. Virtually organized gangs are usually very loosely structured, and their operations often cross national borders and boundaries. The gang members meet and coordinate their activities on the Internet. They also use the Internet to buy and sell goods,” says Neate.

Criminals sometimes use spyware and targeted trojans in their activities to obtain data. Spyware generally refers to software that takes control of a computer’s operation for the gain of a third party. Trojans, on the other hand, refers to innocent-looking programs that are imbedded with information that takes control of computers.

Financial institutions, banks and insurance companies are continuous targets for attempted theft. But these

entities have learned to fight back. Hardware and software that links them to customers are routinely evaluated. Encryption protocols protect personal data by converting passwords and personal identification numbers (PINs) into secure code that is sent over a secure connection. Secret keys decrypt the message sent.

Firewalls and virus protection software help keep networks intruder free. Smart cards have also gained hold as an effective countermeasure against thievery. With their microprocessor capabilities, smart cards allow for enhanced levels of authentication.

But when companies have weak or inadequate security controls, thieves are managing to get hold of personal data when they deal with consumers. Credit card numbers and security codes, in particular, are of interest.

**Banks targeted.** According to some estimates, one-quarter of British companies do not have protection against spyware. Consumers are at particular risk when they deal with small companies that sell their wares online, as only one-third of small enterprises encrypt the data that is transmitted along with the payment traffic. Consumers are wise to carefully verify how companies protect data before they transact business online.

Banks, too, are natural targets, “as that’s where the money is,” goes the old saying. “The banking sector suffers typically from high volume, low value crime. The losses suffered as a result of this type of crime amounted to £ 23 million

(€ 34million) last year,” says **Stephen Bonner**, Director of Technical Security at Barclays Capital.

Criminals sometimes “phish” for personal data by sending emails to bank customers in the bank’s name. Phishing is IT jargon for any one of a variety of ways that criminals attempt to fish, with the “f” turned into “ph,” for personal information (see page 4 for more on “phishing”)

The email generally requests that customers update or verify personal information. Banks have until now agreed to reimburse their customers in these instances and have asked they that report any suspicious email to the banks. Banks also routinely request customers never to answer emails asking them to update or verify personal or account information. Public awareness of what constitutes suspicious activity is thus important in rooting out crime.

**Security measures vital.** Thieves can hide in the most innocuous places. Even the British Salvation Army is not safe against electronic data crime. Such charity organizations collect financial

data from their donors in order to apply for tax refunds on the amounts received. So, even these organizations must protect themselves just like major financial-based institutions.

While digital technology has opened new doors for the trading of products and services in a way that has enhanced the lives of people worldwide, all entities operating this electronic paradigm must view system security as an important cost of doing

business. Just as doors are locked when pet shop owners leave their stores at the end of the day, sellers of pet products online must also lock their computer systems to prevent intruders. Arguably a higher level of sophistication is needed to guard computer systems than is needed to guard a retail outlet. And it is here that purveyors of goods and services are carefully considering the measures that they should take to best safeguard their electronic data. |

“The banking sector suffers typically from high volume, low value crime.”



**Stephen Bonner**  
Director of  
Technical Security  
Barclays Capital

## Information security breaches on the increase

British companies have learned the hard way the importance of investing in security. While 74 percent of British companies suffered information security breaches in 2004, the figure fell to 62 percent in 2005. But, at the same time, the number of attempted breaches of information security has increased.

A study conducted by the Department of Trade and Industry and consultants PricewaterhouseCoopers reveals that currently 4–5% of IT investments relate to investments in security, whereas the corresponding figure for 2002 was only 2 percent.

The survey results showed that the larger the company, the more noticeable was the improvement in security. Major companies have reported a substantial decrease in the cost of data security breaches in the last couple of years.

Yet although breaches of information security are becoming less commonplace, criminals are more determined than ever to tap

into data. Hence an increasing number of companies are reporting attempted break-ins to their Internet or telecommunications systems.

One inference from the report is that there is still room for improvement in information security systems, particularly amongst small and medium-sized companies. Most have virus software and firewalls in place, but many small companies are not protected against spyware and many do not encrypt the data that is transmitted in their payment traffic.

Only one-half of companies using voice over Internet protocols (VOIP) have considered the security risks associated with such calls.

Most of the companies that participated in the study expected to see an increase in the numbers of attempted information security breaches. Companies that conduct financial transactions online naturally attract the greatest number.



# What is a SECURE

In an environment where threats to security are on the rise, it is important to appreciate what the solutions might entail. Some security systems rely on software, others on hardware. The best probably use both – and a dose of good communication.

TEXT Satu Jussila PHOTOS Tommi Tuomi



# solution?

**TO UNDERSTAND** what a secure solution involves, we talked to a systems integrator – someone whose job is to link together all the component parts of the architecture.

“For me, a secure solution has three component parts,” explains **Jeff Demers**, Manager of the Technical Sales Consulting Group for Siemens Communications.

“At the front-end is the user layer. Here, authentication tools, such as smart cards with digital certificates or user IDs with

passwords, come to play. At the back-end is the identity management infrastructure, which involves provisioning, password management and synchronization. In the middle is the network infrastructure, consisting of firewalls, routers, LAN networks and intrusion detection systems.”

Demers says that companies may inadvertently create risk by doing strong authentication at the front-end without equally strong back-end controls. “People may have left the company and still have

access to the system if you rely solely on the front-end.”

In the past, people conducted business with a bricks-and-mortar retail outlet, or on a face-to-face basis with those they knew and with friends-of-friends. The challenge nowadays is finding a way for parties not otherwise known to each other to transact business in an electronic world without even the psychological comfort of face-to-face contact. This is a challenging task and means that parties must trust >



the system design. Trust is critical in an electronic paradigm.

**Customer needs lead.** For Demers, the project begins with his customer. He or she seeks assistance in fulfilling a security need: a secure solution that is easily understandable for the end-user and that fits within budget constraints. The security environment outlined by the customer is reviewed in conjunction with applicable business objectives and government regulations. An assessment is made, among other things, as to the number of users, applications accessed and volume of data within the customer's security environment.

Above all else, Demers wants to make

sure that the solution supports the customer from end-to-end.

"Each vendor or customer has a different approach as to what end-to-end security means. For me, you have to start from the perspective of the end-user," he says. "What tokens does the end-user employ – are they smart cards or other devices?" questions Demers. If the system is too difficult, users will try to find ways to get around it, and this, according to Demers, may ultimately result in a solution that does not deliver its objectives.

"It is the job of the systems integrator to add security for the customer while making it easy for the user," he says. In the past, system integrators worked

solely with technology groups. But this is not enough today, claims Demers. "The system integrator's efforts must include project management and user communication planning if the system is to be successful".

And, most importantly, the system integrator must understand how all the pieces of the digital security puzzle fit together.

**Endpoint security.** Broken down into its elements, endpoint security entails building a system that maintains confidentiality, integrity and authentication. It ensures that while legitimate users find it simple and convenient, unauthorized intruders would need to spend a disproportionately vast amount of time or money to defeat it.

Confidentiality involves mechanisms that prevent access to information by unauthorized persons. It is partly achieved through traditional security means. These involve seemingly simple things like placing computers and discs in a safe environment; careful employee hiring and background screening policies; and avoiding writing down passwords. But it is also achieved through encryption, which generally involves use of message authentication codes (MACs) or digital signatures.

Integrity, on the other hand, means the system ensures that information is not altered by unauthorized persons,

## Endpoint security

Endpoint security entails building a system that maintains:

- > **confidentiality**, by preventing access to unauthorized persons;
- > **integrity**, by ensuring that information is not altered by unauthorized persons; and
- > **authentication**, by ensuring users are whom they claim to be.



or that if altered, authorized users can detect it. Integrity is achieved through checksums, which can involve the use of cryptographic hash functions.

**Authentication** is achieved when the network incorporates at least two of three factors:

1. **something the user possesses**, like a smart card or certificate;
2. **something the user knows**, like a password; and
3. **some kind of physical attribute**, like a person's fingerprint.

Finally, authentication ensures that users are who they claim to be. Authentication is achieved through certificate servers that validate strings of text from encrypted algorithms.

**Smart solutions.** Due to their versatility, smart cards can play a vital role in enabling secure solutions. Cards that are equipped with public key infrastructure (PKI) capabilities are used by governments as a means to retain data confidentiality, while a bank may use smart card technology to prevent the unauthorized modification of information, amongst many other things. Smart cards with biometric capability provide for additional authentication enhancement and can be used in

“It is the job of the systems integrator to add security for the customer while making it easy for the user.”

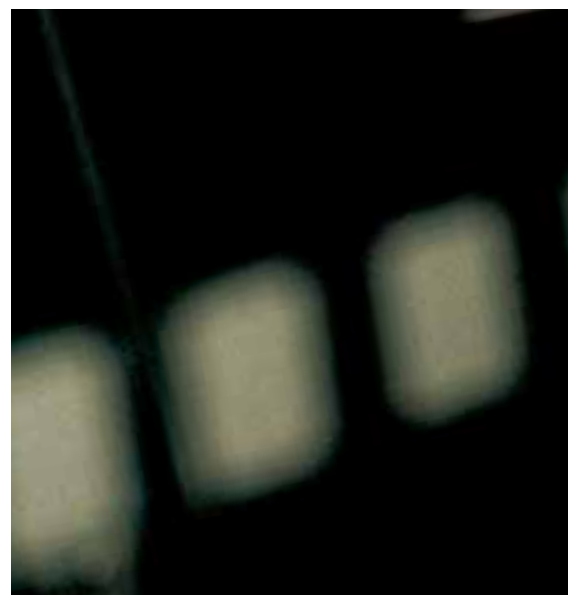
passports to strengthen border control.

But Demers insists that technology is only one part of an endpoint solution. Customers are wise to equip their security environments with a clear security management plan that includes auditing and accountability mechanisms and traditional physical security. Parties need the right mix of policies and user-awareness, in addition to devices.

“A communication plan is also vital”, he says. “It should include a place where employees can go to ask questions and where they can research what is going on.” Demers says that many employees worry about the “Big Brother” aspects

of security. But the truth is that a secure solution ensures that privacy is less impacted.

“Front-line employees are concerned not so much about the business value of the secure solution, but how it will impact them personally,” says Demers. It is important that companies sell the importance of the project to employees and get them on-board. “If you tell your employees, ‘this is what we’re doing and that’s that,’ you risk failure.” Demers encourages companies to have a conversation with employees. “Unless you get the users to trust the system, it will not work.” |



# I love it!

**YOU'RE SITTING WITH A FRIEND** at a busy street-side café for lunch. It's time to pay. Your friend hands in a standard bank card. But you, instead, carefully present a transparent card with a rounded-edge. It's a small thing, in a way — but that quirky card makes you feel good when you hand it to the waiter.

Why should the things that we touch on a daily basis be boring? Why shouldn't a payment card's appearance serve as a personal identifier?

Pastel-colored cards may appeal to women who like to emphasize their femininity while rounded-cornered cards may appeal to young professionals who want to show their originality.

Banks have noticed that distinctive card designs have helped attract customers. Fun designs are sometimes the extra

boost that convinces customers to buy a certain bank's services, as the designs strike a chord with them on a personal level.

Some payment cards have photos or personalized illustrations. The texture, shape and size too can be distinct. Cards have leather or denim-feeling textures and others use plastic with environmentally-friendly holographic imagery — talk about distinct!

Technology surrounds us, and personalization perhaps provides a way to bring seemingly impersonal devices closer to our hearts. As cards take on even greater functionality, this personalization may just help push their use into new areas. |





# A world leader in digital security



## Secure, convenient solutions for identification, communications and transactions

In an increasingly connected, digital world, we need solutions that bring security and freedom to our everyday lives. Whether telephoning, paying, crossing borders, accessing an IT network or our place of work, more than 1 billion of us already benefit from Gemalto's secure personal devices, platforms and services.

Created from the combination of Gemplus and Axalto, Gemalto helps its clients deliver trusted, convenient services to their customers worldwide.

[www.gemalto.com](http://www.gemalto.com)

**gemalto**<sup>\*</sup>  
security to be free