



SECURITY MEETS SIMPLICITY TO CREATE TRUST

AN IDENTITY AND NETWORK AUTHENTICATION
WHITEPAPER FOR DIGITAL SECURITY

INTRODUCTION3

DIGITAL INTERACTIONS IN TODAY'S WORLD3

IMPACT OF INCREASING DIGITAL INTERACTIONS5

DEVELOPMENTS IN THE SECURITY LANDSCAPE13

THE DIGITAL SECURITY CONCEPT15

**GEMALTO'S SOLUTIONS AND SERVICES IN DIGITAL SECURITY FOR
ENTERPRISES AND INTERNET BASED ENTERPRISES16**

Introduction

Digital interactions are a major part of modern life whether in a personal or enterprise setting. These interactions are of increasing importance to both individuals and enterprises while correspondingly coming under greater threat from cybercrime (phishing, pharming etc). This whitepaper looks at the major trends driving these interactions, their impact, and the challenges involved in providing a convenient and secure method for conducting these interactions. It will explore the concept of digital security particularly with regards to securing digital identities, assets and transactions. The whitepaper will focus on the challenges of identity and network authentication and also analyse the related offerings of Gemalto, a leading player in digital security, in these fields.

Digital Interactions in Today's World

In today's world, we are surrounded by digital information whether at home, work or play. This digital information ranges from personal data such as health records, through media files to work documents. These pieces of digital information hardly ever exist in pure isolation; rather they are, more often than not, exchanged/transferred through digital interactions with other people and devices. Digital interactions exist in almost every aspect of modern life, from the way we act as individuals, how we communicate and organise our life, to how modern enterprises and governments function. In enterprises, these digital interactions occurred primarily on the internal corporate IT systems which were used to boost efficiency and productivity. Digital interactions have rapidly become more pervasive and important primarily as a result of the convergence of the following trends:

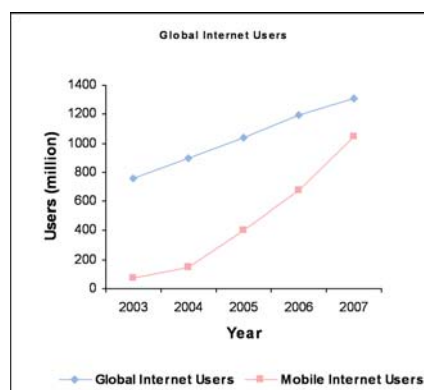
- The rising penetration of the Internet in both the enterprise and consumer space.
- The ubiquity and multiplication of digital devices e.g. mobile phones, flash storage, etc.

By understanding the evolution of these trends we can better understand how the digital world is evolving and the impact on our digital interactions.

The Rise of the Internet

The Internet has rapidly evolved to become one of the most defining technologies of the early 21st century. Rapid user penetration coupled with the ability to radically alter ways of working have been the main drivers. Through its offshoot applications such as the World Wide Web, email and VoIP it is enabling a vast number of digital interactions. According to Frost & Sullivan the number of global Internet users will nearly double from 760m in 2003 to 1.7bn by the end of 2007. The growth is driven by geographic expansion and by alternative modes of access. Particularly,

mobile devices such as PDAs and mobile phones with over a billion users accessing the Internet via mobile devices in 2007 will contribute to the expansion (see Figure I). The growth in users has driven the spread of Internet based applications and services such as Microsoft Live, Sales Force.com, etc



Source: Frost & Sullivan, 2006

Figure I: Global Internet Users 2003 -2007

Impact of Internet Pervasiveness

The growth in Internet penetration will enable individuals and organisations to access share and deploy digital information and services globally. The rise in mobile Internet access will add to the benefits of using the Internet making digital information available "any time and anywhere".

Ubiquity of Digital Devices

The convenience of digital interactions is supported by an ever increasing array of advanced digital devices. These devices have become the cornerstone of modern life, particularly in the areas of:

- Computing e.g. personal computers, laptops;
- Communications e.g. mobile phones, pagers; and
- Entertainment e.g. video devices and media systems.

Communications devices have evolved from basic usage towards computing and entertainment. This is demonstrated by the modern generation of mobile phones, which can act as MP3 players, access the Internet through 2.5 and 3G networks, and play video content. Likewise, traditional entertainment systems such as DVD players, audio systems are also being expanded in their computing and communication capabilities e.g. current generation of home media centres and Apple TV. The cross functionality of devices facilitates an increasing range of digital interactions even on the same device.

Of particular interest is the development of the mobile handheld devices¹. These devices (along with laptops) provide the additional benefit of mobility enabling digital interactions in a wider range of locations and situations. In 2006 alone, around a billion mobile handsets were shipped globally. This proliferation is expected to continue in the future leading to mobile handset devices becoming important means of digital interaction globally.

Impact of Device ubiquity

Digital devices are increasingly supporting more diverse digital interactions. Flexibility in the use and management of digital assets e.g. the transfer of digital media from the Internet to a home storage system, or to a portable media player has become not only a digital right management issue but also a security issue. If a malicious program such as a virus or Trojan finds its way onto one digital device it can be very easy for it to spread to others.

¹ These include mobile phones, smart phones and PDAs

Impact of Increasing Digital Interactions

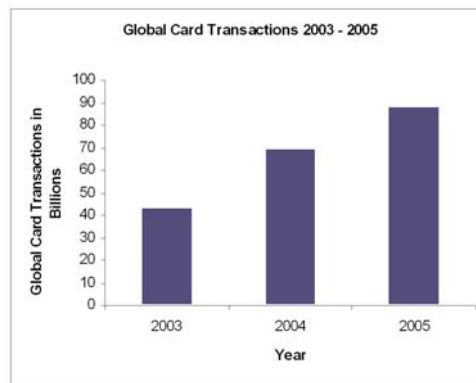
Proliferation of networked digital devices is becoming ever more common. As a result, we are able to engage in more digital interactions through an ever expanding number of options. The increase has led to the evolution and in some cases revolution of individual and business practices world wide.

Impact on Individual

The average individual now spends more time online than ever before, connected through an array of digital devices. We are now conducting a significant proportion of our every day transactions (see Figure II) through new digital mediums such as:

- Online retail.
- Mobile payments.
- Online tax filing.

The convenience made available through digital interactions has been the main driver for their adoption. These digital interactions require more of our personal information such as credit card details, bank account details and address information to be available digitally. These pieces of information which form one's digital identity can at any point in time be stored or transferred through an array of devices from laptops to mobile phones to payment cards. If a device is lost or stolen then an increasing amount of sensitive information becomes under threat. Typically user logins and/or device passwords and Personal Identification Numbers (PINs) have been used to secure these devices. However, keeping track of multiple IDs and passwords for different devices and services becomes a difficulty for individuals e.g. if a person has to type a PIN to access a mobile phone, then another password when wanting to access email. **It is critical to find more advanced, secure and convenient solutions for identification and access other than passwords.**



Source: VISA, 2006

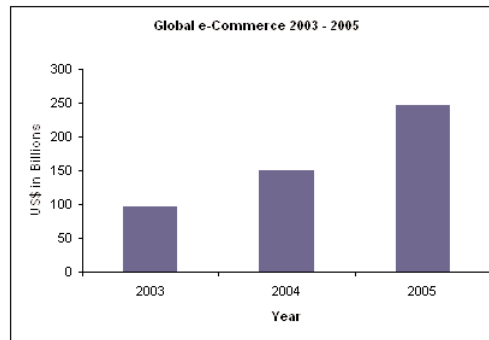
Figure II Global Online Card Transactions 2003 to 2005

The Security Perspective

Consumers are concerned about misuse of their personal details both online and in the physical space. In fact, 48% of UK consumers do not feel confident about the security for mobile banking and 73% think that protection of personal details is their main criteria when buying online (LogicaCMG, 2006).

Impact on Private Enterprises and Public Sector Organisations

Both private enterprises and public sector organisations are becoming ever more dependent on digital communication and processes in their interactions with customers/users, employees and other organisations. More companies are using the Internet as a channel to market, leading to the rise in e-commerce transactions from \$96 billion in 2003 to \$246 billion in 2005² (see Figure III). The increase in mobile networked devices has enabled organisations to implement new ways of working such as remote working and field mobility.



Source: See footnote 2

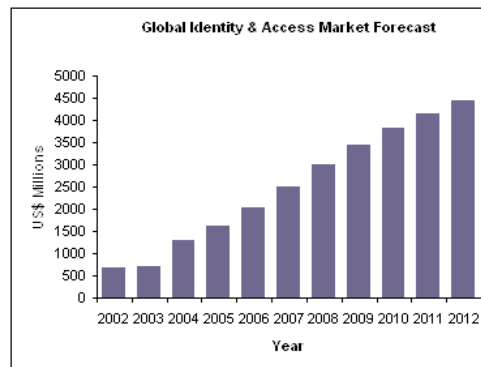
Figure III Global E-commerce Transactions
2003 to 2005

These new working practices and processes effectively shift core business systems, data and applications onto a wide range of devices.

As a result, devices that are insufficiently secured pose a huge risk in the hands of an unauthorised person, as they will be able to access personal information and potentially an employer's core business system.

Managing Identities and Access

The increased dependency on communications networks means that more and more critical information is ending up stored and/or transferred on company networks and IT systems. This has made it imperative to have identification and access management for these networks and systems. As a result, the identity and access management market grew by 193% between 2002 and 2006 to \$2 billion. The market is forecasted to grow by 119% between 2006 and 2012³ to \$4.4 billion.



Source Frost & Sullivan 2005

Figure IV: Global Identity & Access Market
Revenue from 2002 to 2012

The rise in the Internet and mobile devices has made it possible to work from any location. This has enabled the sharing of applications between employees in different locations, and provided opportunity for efficient communication despite geographical distance.

Irrespective of the employees location the control and management of access to the system must be highly secure. This has traditionally been attempted through the use of login names and passwords. Having yet another password added to the many other online passwords an employee must remember may cause confusion. Employees are more likely to compromise security when it is inconvenient despite company policies on the matter. It has been argued by vendors such as Novell that passwords alone are actually a less cost efficient method of securing identification, and access than previously thought. This is primarily due to the fact that IT departments often spend more time than anticipated on retrieving employee passwords, or ordering new ones.

² Source: Visa and Frost & Sullivan estimates

³ Frost & Sullivan, 2006

Remote Security

Convenient and secure identification and access has become an ever more important and larger challenge due to the increase of advanced mobile devices such as laptops, PDAs and smart phones. Likewise, the applications being developed for these devices such as MySAP Mobile, which allows Sales Managers to approve invoices over their mobile, are also becoming ever more advanced and integrated with companies' core business systems. It is therefore, necessary for the corporate IT department to support these devices, and ensure that they are compliant with security policy.

The increased remote access to the network also means increased exposure of the system. Therefore, some enterprises have deployed Secure Socket Layer (SSL) and Virtual Private Networks (VPN) solutions to enhance security especially taking into consideration their remote workers. Corporate security policies typically require that the appropriate anti virus and anti spyware software are installed on devices connected to the corporate network.

To meet both the demand for convenience and heightened security some companies such as banks have biometric solutions. Employees on the trading floors will have to touch a pad to provide fingerprint identification to access a system and/or an area.

Convenient and Secure Physical and Logical Access

Private enterprises such as banks and public sector organisations are also concerned about controlling physical access to high security areas in their facilities such as server rooms. Presently technologies such as voice recognition technology and whole body scanning are being used for physical access control. Given the needs for controlling both physical and logical access to systems and facilities the ideal access solution would hold identification and access details for both forms access.

In the public sector, governments across the world are in the process of introducing biometric passports some requiring fingerprinting or retina scanning to ensure a convenient identification and access control. Biometric solutions provide a convenient and secure option but can be more expensive as the technology is relatively new and there is a need for deploying the corresponding infrastructure such as iris scanners. For Biometric solutions to be more cost efficient they must be deployed over large scale.

Governments and some large enterprises have introduced smart cards as corporate IDs. Smart cards are both highly secure and convenient. The employee does not have to remember any passwords, just a single PIN. A quick push into the reader is even more convenient than having to enter a password. Furthermore, the information on the smart cards can be encrypted making this a highly secure option. However, there may be higher initial cost than with password solutions as readers have to be deployed. In the personal computing space vendors are increasingly integrating smart card readers into their new models. A trend we expect to continue as hardware costs drop and software solutions that can take advantage of the technology become more widespread e.g. with the expected penetration of Windows Vista.

In the mass transit area, various smart card based solutions such as Hong Kong's Octopus card, London's Oyster Card, generally have very high acceptance among citizens and consumers. Another advantage is that smart cards like biometrics can be deployed for both physical and logical access.

Impact on Internet Based Enterprises

The evolution and proliferation of the Internet has enabled access to a larger number of services more conveniently. An example of such behaviour is demonstrated by the 156% increase in the value of e-commerce transactions from 2003 to 2005, to \$246 billion. Simultaneously, as people become more accustomed to Internet usage their demand for more advanced services and content increases.

Internet based enterprises offer customers a convenient alternative for their digital interactions. The consumer can execute a wide range of transactions in the comfort of their own home as opposed to previously where they would have had to go to a bank or a store.

While interacting on the Internet people have become more familiar with the large Internet Based Enterprises (IBEs).

IBEs are companies which sell, buy or provide services online. There are several types of IBEs:

- Online retailers, who sell and/or buy products and services exclusively online such as Amazon, or e-bay which also owns the secure online payment company PayPal.
- Enterprises with online capabilities such as Wal-Mart, Citibank, Financial Times, Singapore Airlines, etc. which have a physical operation along with an Internet operation.
- Social networking sites where people can meet or stay in contact with existing social network such as MSN Messenger, Friendster or dating sites such as Match.com. Some of these sites are developing into reality entertainment channels such as YouTube or My Space.
- Web based email services such as Yahoo Mail, Google Mail and Microsoft Hotmail.
- Portals and search engines such as Google and Yahoo.

These companies have managed to provide robust, reliable, and relevant services and thereby gained consumer's trust and confidence.

These IBEs succeed by providing their customers with an ever increasing portfolio of advanced services. These services often cut across social and transactional areas/functions e.g. eBay/PayPal/Skype (Skype chat and Skype out) MSN passport/messenger, Yahoo messenger/wallet. Companies like Microsoft, Google, eBay and Amazon benefit from being able to provide users

Accounts Globally (millions) ⁴	2006	2005	2004
Online Retailers: eBay	181	135	72
Social Networking: Messenger Skype	240	180 95	145 33
Web Mail: Hotmail Yahoo Mail	270	228 379	187 250

Table 1: Growth of Internet Based Enterprises

with tailored services/experiences e.g. Amazon tracks user purchasing behaviour to make purchase recommendations. As a result, consumers end up providing an increasing amount of information. This information is used not only for security but also to allow companies to enhance their customer relationship management (CRM) in terms of cross selling, up selling, and product development. As a result, IBEs hold an increasing amount of personal information. Therefore, it is business critical to gain and maintain the trust of their customers by "proving" high security standards to enhance their business.

⁴ Source: eBay, 2006; Microsoft, 2005, and 2006; Guardian, 2007; and Info World, 2006

The same individual is likely to use the Internet for many different functions ranging from social interaction to interacting with the public sector organisations. Therefore, **the average individual holds approximately 20 different online accounts for online banking, Internet based email, several social networks, several online retailers, etc**⁵. As a result, it becomes difficult and confusing for consumers to remember all their logins and passwords. To avoid confusion, many write their details down and thereby compromise security. As an alternative many end up saving their password and login name on their devices, which can still compromise security in the event of their devices being lost or stolen.

IBEs also have to contend with a growing range of cybercrime threats focussed specifically at the services they offer. These threats include sophisticated social engineering as in phishing and advanced programs such as spyware which are designed to unlawfully access and manipulate IBE customer information.

As new threats arise consumers are becoming ever more concerned about the safety of their personal and payment details. According to research by eBay 65% of consumers globally are concerned about identity theft, and 60% about theft of their bank account information and 59% about theft of their credit card details when purchasing online⁶. In fact, according to research conducted by LogicaCMG 65% of UK consumers said they would never purchase from an online retailer who experienced security breaches.

As a result, there is a clear need for more effective and convenient identity and access security solutions.

⁵ Source BBC Click Online News Report 9th February 2007

⁶ eBay Analyst Day 2006

Changing the Face of Communication

The Internet has transformed the way we communicate. Digital communication has provided convenient ways to stay in touch with friends and relatives at affordable cost despite geographical distance. As a result, Internet based email accounts such as Hotmail have shown amazing growth rates of 44.4% from 2004 to 2006 globally. Digital communication has also brought new ways of interacting and extending social networks. It has become just as common for teenagers to hang out with their friends on MSN Messenger or Friendster.

Therefore, people have an increasing amount of social network accounts with different passwords making it confusing to remember. Furthermore, people have personal information stored on these sites. To protect access and avoid unauthorised access to these accounts passwords and logins are required.

Just as digital communication has provided easier access to sustain and expand social networks. It has also enhanced business opportunities by enabling buyers and sellers to engage despite geographical distance thereby providing direct access to the global market.

Digital Interaction Meets the Public Sector

The e-government, e-health, and homeland security initiatives launched in many countries vary depending on the country's culture and existing public sector processes. However, they will have one thing in common; public sector organisations will hold more information about citizens. In many countries, such as the UK, this is based on a longer-term aim of providing "one view" of each citizen.

Furthermore, increased digital interaction between the citizens and public sector organisations are also among the common goals. In many cases, this will include: electronic voting, electronic filling and payment of taxes. As a result, each citizen needs a secure and trustworthy method of validating his or her identity in relation to their interactions with public sector organisations e.g. in electronic voting.

To ensure secure authentication, access and payment an alternative solution to basic passwords is needed just as it would be the case with commercial IBEs.

In certain countries such as Denmark the Government has enabled the use of digital signatures, which can be used for interactions that would usually require a physical signature. The digital signature works as a certificate, which is installed on the citizen's device. Digital signatures may also enhance the payment security, if for instance a signature was required to processes the transaction.

Digital signatures are despite their convenient usage and secure form of identification not able to fully address current threats. They are currently mostly utilised in the public sector where it can be a useful tool in relation to for instance e-voting.

Furthermore, there are not yet clear guidelines for when a digital signature is equivalent to a hand written signature. This may have to be established in many countries before uptake becomes mainstream and widely utilised for commercial purposes as well.

Identity Threat

With so many organisations involved in these public sector initiatives there is the threat of unauthorised groups or individuals accessing databases and exploiting the sensitive personal information stored for criminal/malicious means.

Reaping the Benefits of Digital Interactions in E-Commerce

E-commerce sites have enabled people to reap the financial benefits of digital interactions through being able to expand customer base despite geographical distance. Sites like e-bay have dramatically increased their number of users by 151% from 2004 to 2006 globally.

For consumers to be able to shop and bank online they will be required to set up a profile with personal information. In most cases, this profile will be linked to the purchases and the searches the individual makes. As a result, these sites store increasingly larger amounts of personal information such as name, address, telephone number, date of birth along with credit card details. Essentially, all the information a malicious person needs to conduct transactions in another individual's name or steal from a banking account. Therefore, it is critical for consumers that online identification, access, and payment processes are secure. According to research conducted by LogicaCMG 73% of UK consumers says that security is their main criteria when using Internet based services.

In an attempt to meet this concern, card operators like VISA and MasterCard have introduced secure online payment programs such as "Verified by VISA", and "MasterCard SecureCode".

Online banking is becoming increasingly popular due to the convenience it provides. In the US the number of online banking users grew by 385% between 2002 and 2005 to 63m users⁷. Furthermore, in the UK 98% of online banking users also have online credit card accounts, and 90% of UK online banking users also having at least one online retail account (Apacs, 2006). As a result, secure online payment has become a priority for banks and retailers. In an attempt, to enhance security Barclays bank in the UK has started to offer their online banking account holders free antivirus and anti spyware software along with two factor authentication. Other banks such as Lloyd's TSB have started to experiment with tokens and other hardware authentication methods.

Consumers in the UK are concerned about online security. Up to 2% have stopped using online banking because they are scared of identity theft and spyware (Apacs, 2006). As a result, banks are facing a challenge to enhance consumer confidence to be able to further increase online banking penetration. Furthermore, confidence in the banks online offers is necessary to support the penetration of new routes to market such as mobile banking and contactless payment.

There is a clear need for IBEs, banks and public sector organisations to retain trust in their brands and channels to ensure increase in penetration of online offers. As a result, it has become business critical for them to proactively show consumers that they are enhancing security of their identity, access, and their payment processes.

The Verified by VISA program has become very popular with both consumers and retailers. The program increased the number of card holders globally by 80% from 15m to 27m between 2004 and 2005 highlighting the great demand for secure online payment.

⁷ Pew Internet & American Life Project, 2006

Creating Secure and Convenient Interactions

There are two main reasons for concern over the current identification and authentication methods namely:

Confidence: It is generally accepted that the use of username and password combinations alone no longer provide an effective method of identification. Therefore, consumers will need to be presented with alternative methods of authentication and access tools along with secure payment processes in order to maintain current growth trends. This is supported by research conducted by RSA which suggests that 73% of consumers globally would prefer their bank to deploy new authentication methods such as hardware tokens. Consumers want to be assured that when they log into their account they are in fact transferred to the actual site and not a fake one designed to steal their personal information or clear their credit card. Consumers have now realised that no matter the device used (desktop, laptop, PDA or mobile phone) there exists a growing range of security threats. The very benefits of being able to connect to the Internet through multiple devices are under threat from security threats faced by these devices.

IBEs have to ensure consumer confidence in their service in order to ensure growth. By continuously providing secure identification, access and potentially payment the IBEs reduce security concerns and enhance confidence in their services. Furthermore, if consumers are made aware of extra steps taken to enhance security, the confidence will be translated into trust in the brand.

Convenience: There is a huge need for making the authentication and access methods more convenient, and at the same time increase security. Since it is almost impossible for an individual to remember the high number of different passwords, it causes confusion. The confusion would become further exacerbated if each IBE was to introduce its own new token, and/or other security hardware solutions in the attempt of enhancing security. The inconvenience of having to walk around with multiple hardware devices is likely to make consumers compromise on the extra security measures making them almost redundant.

Due to the confusion of the many passwords and the impossible task of remembering all of them, many consumers save passwords and logins on the server. Alternatively, some write passwords and login names down. Some even write them on Posted Notes attached to the screen such compromising the security even further.

Moreover, many forget their passwords, and the IBE has extra cost in retaining passwords or providing users with new ones.

The challenge is as such to find a solution that ensures:

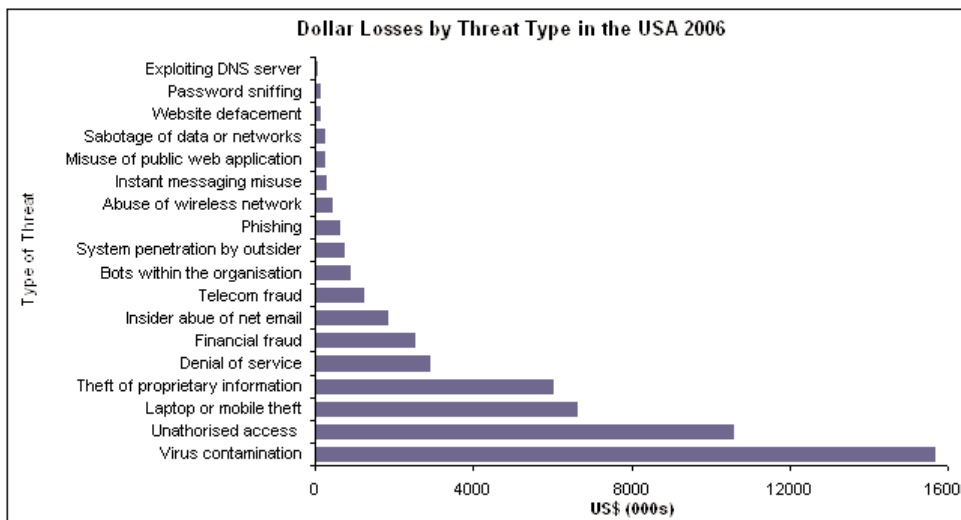
- One "global" password/PIN code.
- A convenient and secure method to store passwords.
- A secure log in process so the consumer is assured they are directed to the right site when typing in passwords and login details.

The ideal solution should be convenient for the consumer to use; otherwise as experience has shown that security will be compromised. At the same time the solution should enhance consumer confidence in the IBE brand by protecting the consumer against the wide range of threats such as phishing, pharming, password snooping and keystroke logging.

Developments in the Security Landscape

The increasing dependence of consumers and organisations on digital information has presented new opportunities for cybercrime. Historically, cybercrime has been perceived to be mainly about virus attacks and network hacking. Though these still form the mainstay of attacks, new forms such as phishing, fraud and digital identity theft are on the increase. In its 2006 cybercrime survey Symantec discovered that there was an 85% increase in phishing messages detected in the first 6 months of 2006 over the equivalent period in 2005 (157,477 to 97,592 messages respectively). In the UK alone the losses from phishing have increased 927% in value from £4.5 million in 2004 to £45.7 million in 2006⁸.

Additionally, threats to devices have become more important. The 2006 CSI/FBI survey noted that in the US, losses from laptop or mobile hardware theft increased from \$19,562 per respondent in 2005 to \$30,057 per respondent in 2006. This is in contrast to the general trend of losses from security incidents reducing⁹ and reflects the increased value of the information being stored on these devices. The second of only three areas which experienced an increase was telecoms fraud. This increased dramatically from \$2,750 per respondent in 2005 to \$12,377 per respondent in 2006. The overall losses incurred by respondents across the incident categories are shown in Figure V.



Source: CSI/FBI, 2006

Figure V: US Enterprise Losses from Security Incidents

It is also worth noting the high cost of unauthorised access to information as it demonstrates the impact of the loss of ones digital assets.

Cybercrime is also extending to new devices; the proliferation of handsets with Internet capabilities has provided cybercrime attackers with new attack opportunities. Most notable has been the growth of mobile malware for which there are currently over 220 known variants up from a base of 1 in Q2 2004.

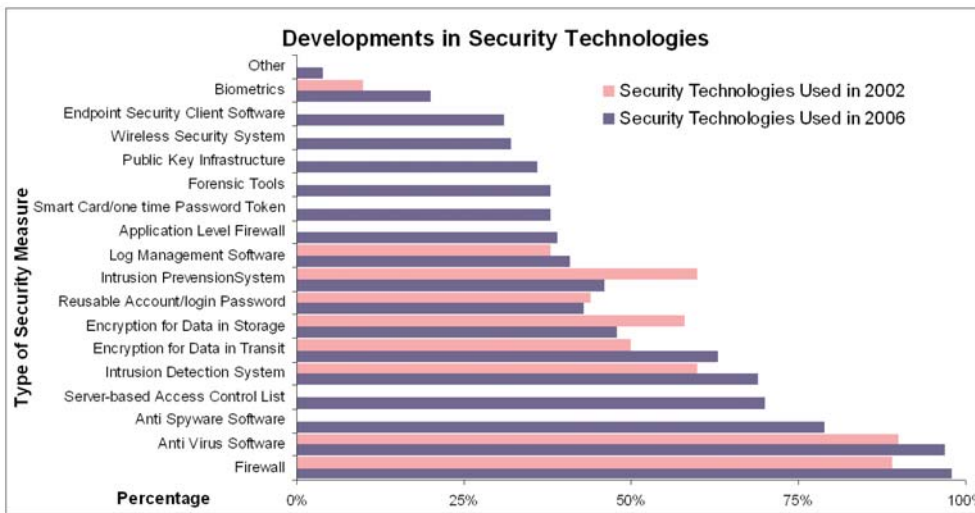
⁸ Financial Services Authority, 2006

⁹ The third category in which average losses increased was Web site defacement. While the average losses for this category increased from \$1,494 per respondent to \$1,806 per respondent, less than one-third of a percent of total losses reported were due to Web site defacement.

Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. As phishing attacks grow it will become increasingly important to be able to guarantee digital identities.

Individuals and enterprises have traditionally responded to cybercrime using the staple tools of firewalls and antivirus solutions. However, as the new threats, evolve both individuals and enterprises are finding that new innovative solutions are required to overcome threats. Some of the ways in which they do so are as reflected in their implementation of new applications as shown in Figure VI.



Source: CSII/FBI, 2006 and 2002

Figure VI: Enterprise Implementation of Security Technologies 2002 to 2006

Of particular interest is the increasing focus on securing digital devices in terms of end point security, digital identities and access (Smart card/Tokens). The use of these technologies represents an acknowledgement of the need to expand the focus of security beyond the core of enterprise networks. As global and remote working become more common place enterprises will face the challenge of securing employee digital interactions, no matter the location or access device.

Market opportunities in Biometrics and Hardware Authentication

According to our research there is a significant growth opportunity in the Biometrics and Hardware authentication markets. The markets for finger print technology and iris recognition technologies are forecasted to grow from \$393 million in 2006 to \$1.1 billion in 2011. In the same time frame hardware authentication is expected to grow from \$396 million to \$1.2 billion.

The Digital Security Concept

As more digital devices are interconnected and allow users to perform additional tasks, the role of users in a digital world is likely to change. Any device, anywhere, anytime access is increasingly demanded and this has clear security implications. User identities and personal information are at risk and on many occasions, digital devices overlook the security implications. However, digital security is a concept that is evolving. At present, we are on the way to a world where information is becoming increasingly available through an array of different digital devices. However, the threat of malicious third parties looking to steal user identities and gain unauthorised access to confidential data and resources is also increasing.

In order to get to a successful digital world, the use and implementation of dedicated security technology is required. This security technology needs to protect the assets and identities of the digital users but also needs to be user friendly and convenient. Ultimately, all digital devices will be able to connect with each other, offering users the possibility to interact with other users and access any type of information from their digital devices, safely and conveniently. This way, digital users will feel confident to perform any type of transactions from their digital devices as security will come as a given.

Secure protection of digital identities, assets, and transactions is vital for individuals, enterprises and public sector organisations. Equally important, is the users' sense of ease and confidence in entering into digital interactions. Digital security can therefore be simply defined as the solutions that protect and enhance digital identities, assets and interactions, based on a combination of secure personal devices, software platforms, and services.

Gemalto is one of the companies that are leading the way towards the enablement of a secure digital world. Created from the June 2006 merger of Axalto and Gemplus, Gemalto provides end-to-end digital security solutions. Its offerings range from:

- The development of software applications, including embedded and non-embedded software, middleware, and server-based solutions;
- The design, production and personalization of secure personal devices such as smart cards (including SIM cards), e-passports, and authentication tokens; and
- The management of deployment services for its customers.

Its key markets include the telecommunications industry, the financial services, retail markets, enterprise customers, Internet based enterprises, public sector agencies, and mass transport operators.

In the Identity and Access management space, Gemalto's recent main offerings are:

1. The Network Identity Manager (NIM) a USB device for secure online mutual authentication; and
2. The .Net card a smartcard based solution for physical and logical access control.

Both offerings are analysed in detail in the following section. These two solutions highlight the new direction of Gemalto into providing digital security; a strategy that we feel recognises the increasing importance of securing digital interactions in today's world.

This strategy will ultimately take Gemalto into a wider range of activities and new offerings around: secure personal devices (e.g. microprocessor based tokens like cards, USB drives or ePassports) and comprehensive software and managed service solutions.

Frost and Sullivan believes this new strategy for Gemalto will enable it position itself successfully as a leader in the evolving market for digital security.

Gemalto's Solutions and Services in Digital Security for Enterprises and Internet Based Enterprises

An important part of the technology required for Digital Security is classified under the identity and access management (IAM) umbrella. Digital security solutions must expand beyond traditional IT security however to encompass many other areas. These areas include subscriber management and data or transaction protection for applications in telecommunications, multimedia, financial services, and citizen identity. Gemalto is one of the leading players in these market segments. In the following, we will focus on how Gemalto is positioning within the enterprise and IBE space.

In the enterprise and Internet Content Providers markets Gemalto offers a range of IAM solutions such as USB keys and one-time-password tokens; B2B authentication and digital signatures; components for end-to-end security solutions, including readers, client middleware, card management system, related services and training and access control for buildings, email, IT networks, corporate databases, employee services, benefit schemes, secure project databases and other applications. Gemalto tailors its offerings to address both large S&P 500 enterprises as well as SMBs via its indirect reseller network. Furthermore, Gemalto's corporate access badge solutions are implemented by numerous government agencies worldwide.

Network Identity Manager (NIM)

Gemalto's Network Identity Manager (NIM) is a consumer solution offered through service providers. It is a smart card, browser-based strong authentication system that connects via a USB security device. The user communicates with the smart card USB device through a Web browser and is authenticated to the device by entering a PIN.

NIM mutually authenticates the user and server through an encrypted end-to-end connection using standard security protocols and validates the relying party's public key and URL to values stored on the user's device.

Users can securely login to a remote server knowing their personal information remains private and that they are protected against password snooping, keyboard logging, spoofing, phishing, pharming, man-in-the-middle and Trojan attacks.

Key Differentiating Factors

Ease of deployment

NIM does not require additional server hardware, middleware or any client software on the user's PC. This places NIM ahead of competing solutions that require software updates or the installation of client software that consumers are not always savvy enough to use correctly. In addition, it does not require any administrative rights to operate on the user's PC.

Mutual trust

NIM verifies that the user and the server are legitimate, therefore providing a trusted communication between the consumer and online merchant. NIM verifies that the site is genuine and signs the data going to the server. Then the server verifies the device identity. Only the intended server can decrypt the message.

Strong security without compromising convenience

NIM gives consumers a strong authentication solution that provides a secure connection with the online merchant with the convenience and portability of a USB device that can be used from any PC with a browser. NIM works with standard account privileges and browser settings and the same device authenticates the user to multiple sites.

Cost savings

The format and architecture of NIM allows multiple transaction partners use the same end-user device. This can translate into important cost savings.

Conclusion

Frost & Sullivan believes that Gemalto has launched an innovative and user friendly consumer authentication solution that is convenient and offers the adequate level of security to conduct online transactions.

Frost & Sullivan believes that the use of NIM can minimise the security concerns that many consumers have when making online transactions, as they have the guarantee that they are dealing with a trusted online party through a secure connection. Likewise, the merchant has the guarantee that it is dealing with a legitimate user. Ultimately, this is likely to increase user trust on the Internet as a medium to conduct their purchases, with the subsequent benefits this has for all parties.

Gemalto .NET solutions

The Solution

The Gemalto .NET solution is a smart card system that provides strong authentication for enterprise customers that works seamlessly under the Microsoft .NET environment and service-oriented architectures. The solution is made of several components, including the smart card, the reader and dedicated software.

Gemalto's .NET solution provides two-factor authentication, full cryptographic capabilities and support for on-card applications and services within the Windows environment.

Key Differentiating Factors

Multiple uses

The smart card can be used as a second factor to secure access to buildings, desktops or networks, hold digital certificates to confirm identities and sign or encrypt email and documents.

Strong user security

Gemalto's .NET solution provides both on and off-card application verification. In addition, the security built into the card ensures integrity and authenticity of user.

Tighter user control

The use of Gemalto's card allows organisations to provide an adequate access tool to employees based on the role they perform. This ensures that the right users have access to the right applications and resources.

Quick and seamless integration and deployment

One of the strongest differentiators for Gemalto's .NET smart card is its integrated support into Windows Vista. This makes Gemalto's smart cards easy to deploy and seamless to use without requiring any additional software installation. The same support is also available by download from the Microsoft Download Centre for 2000, XP and Server 2003.

In addition, Microsoft Identity Lifecycle Manager (ILM) also supports the Gemalto .NET card.

Unified communications enabler

The use of .NET Remoting mechanisms for communication between smart cards and a host device simplifies the integration of smart cards within .NET infrastructures and devices. Because of the neutrality of its protocols, it enables emerging application architectures such as web services to be implemented.

Conclusion

Frost & Sullivan believes that Gemalto's .Net smart card system provides an excellent opportunity for businesses running a Windows environment, to implement a multi-use, strong authentication solution that is easy to use, easy to deploy and offers a high level of security.

Increasingly, the convergence of physical and logical access makes Gemalto's .NET solution, one of the best solutions in the marketplace to bridge this gap.

The Smart Microsoft Security Solution

The Challenge

Microsoft is the world's largest software vendor. The company provides innovative solutions for both enterprises and consumers in a wide range of areas from gaming consoles, office applications, software development tools, communication tools, operating systems, etc.

Microsoft was keen to find a robust and efficient authentication solution for identification and access to their corporate network. Furthermore, the company is highly dependent on keeping its research and development activities as well as marketing private until launch. Therefore, Microsoft was also interested in finding a solution that could combat the threat of physical unauthorised access to their premises.

To meet Microsoft's demand for a robust and convenient security solution, they partnered with the global digital security vendor Gemalto. Microsoft and Gemalto developed a solution to meet the threat of unauthorised access to Microsoft's corporate network.

The Smart Solution

Gemalto and Microsoft developed a solution based on smart cards with .NET software. The smart cards were distributed to all Microsoft employees starting in 2002. The solution has significantly increased the security in identification and access to the Microsoft corporate network and physical premises.

The high capacity smart card controls logical access through a microprocessor contact smart card with specialised security features defined by Microsoft themselves. The solution is compatible with all programming languages. Furthermore, a contactless feature was embedded in the card to provide physical access to Microsoft's premises.

The benefits of the solution include:

- Lower risk of confidential information being stolen by unauthorised users.
- Easier administration and control of user access to both corporate network and physical premises.
- More convenient solution for users which should result in employees not compromising security by writing passwords down.
- Increased flexibility and efficiency by having a security solution enabling employees to work wherever convenient.

The .NET smart card is a convenient and flexible way to achieve a high level of both physical and logical security. In addition, the solution supports more efficient and effective working. It enables employees to work from any destination whether that is the airport, home, train or hotel without compromising security. Furthermore, the convenient element of the solution should enable Microsoft to cut cost. There tends to be a higher amount of hours than often anticipated spent on supporting passwords or managing access to physical premises. The digitally centralised administration of the .NET smart card solution requires less time than having to retrieve passwords, having new keys made, or locks changed.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 enterprises, emerging enterprises and the investment community by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics and demographics. For more information on Frost & Sullivan visit <http://www.frost.com>.

Copyright

All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied or otherwise reproduced without the written approval of Frost & Sullivan.