Smart Cards

The use of “intelligent plastic” for access control

White Paper

Bob Walder

First published September 1997

Published by The NSS Group
Network House, PO Box 297, Bedford, MK44 1YR, England

Tel. +44 (0)1933 413636
Fax. +44 (0)1933 359021
E-mail : NSSinfo@NSS.brand.co.uk
Internet : www.NSS.brand.co.uk

TABLE OF CONTENTS

The NSS Group

The NSS Group is the UK's foremost independent network testing facility and consultancy organization - an organization devoted to the needs of the networking professional.

Based in Bedfordshire, England (also with offices and testing facilities in France), The NSS Group offers a range of specialist IT and networking services to vendors and end-user organizations throughout Europe and the United States.

The Group consists of six wholly owned subsidiaries :

- *Network Subscription Service*
- *NSS Consultancy Services*
- *NSS Network Testing Laboratories*
- *NSS Editorial Services*
- *NSS Training*
- *NSS Computers*

Network Subscription Service - the publishing arm of the Group - offers an independent information service providing detailed quarterly reports and monthly newsletters on the latest network-related technologies. **NSS Network Testing Laboratories** services the testing requirements of the Subscription Service as well as offering its facilities and expertise to third parties for private commissions.

The Groups remaining subsidiary companies provide **consultancy services** (including network design, Internet/intranet connectivity and security audits), **technical writing**, **training** (both technical and business oriented), and **hardware**.

Bob Walder

Bob Walder is one of the founders of the company, and remains active both as owner and as one of its principal consultants.

His unique insight into the computer industry in general, and the problems facing network managers in particular, is born from considerable experience in the end-user environment. For eleven years, Bob worked at the “sharp end” of the industry, undertaking key roles in a range of different environments, including a computer vendor and software house, local government, manufacturing, and financial institutions. His final years in industry were as Group IT Manager of a large multi-site manufacturing organization.

Since forming ***NSS*** in 1991, Bob has helped many organizations with their networking problems and strategies. His broad range of expertise has allowed him to contribute to projects, which have involved business process re-engineering, hardware and software selection, NOS migration and integration, and Internet connectivity and security.

He is also regularly involved in independent testing and benchmarking operations for both end-user organizations and network vendors, which are carried out from the extensively equipped ***NSS*** labs in England and France.

INTRODUCTION

As we rush headlong into the information age, we begin to feel as though our very being is defined by a record on a computer somewhere.

Can we drive a car? Can we get a bank loan? Can we borrow a library book? What are our buying preferences? Can we leave or enter the country? Can we get through the front door at our place of work? All of these questions are answered by a quick search on somebody's database.

One of the biggest problems we face as individuals in the information age is the bulging wallet or purse. Unless we are very lucky, however, it does not bulge with cash, but rather with the numerous bits of plastic and paper we have to carry with us on a daily basis in order to prove our entitlement to the above rights and privileges.

Most of us had just about got used to the idea of carrying round one or two credit cards, a driving license, a library card, our employer's ID card and our passport or national ID card when travelling. As if this were not enough, we are now bombarded with "customer loyalty" cards from shops, petrol stations and supermarkets. If we use these outlets regularly, it makes sense to take advantage of these schemes in order to save money, but the real estate it takes up in our pockets and handbags is really getting beyond a joke.

I dream of the day when I can carry a single card with me. A card which will allow me to make purchases (both as a credit and a debit card – maybe even using "electronic cash"), borrow a library book, make a phone call, gain access to my place of work, participate in a few well-chosen store loyalty schemes, and contains all my driving license, passport, National Insurance, personnel and medical records.

As far-fetched as this dream may sound, we already have the technology to do this – it is called a smart card.

WHAT IS A SMART CARD?

A smart card is similar in appearance to a standard credit card, both in size and choice of material. However, instead of the magnetic stripe on the reverse of a credit card, the smart card sports a small gold-colored computer chip approximately one centimeter square. Such cards can also come in smaller sizes – basically just the computer chip on a plastic base – for use in cellular telephones. ISO standard 7816 defines the physical and logical features of smart cards, such as shape, position of contacts, their functions at the user interface, and their file structure.

Depending on the designated function of the smart card, the on-board chip can consist of anything from simple EPROM memory (i.e. in the case of a telephone card) to a full-blown tamper-proof "computer-on-a-chip", including an 8-bit microprocessor, RAM, ROM and EEPROM.

Contact Cards

When the card is inserted into a smart card reader (or telephone), it makes contact with electrical connectors that transfer data to and from the chip. Data written to the card can be stored either in the RAM or EEPROM, with the ROM used purely to store the microprocessor's operating system.

Whilst the RAM is used primarily as temporary work space for the on-board applications, the EEPROM is designed as a more permanent (though re-writeable) form of storage. Like the hard disk on a PC, the EEPROM provides a hierarchical file structure on which can be stored critical data (such as PIN numbers or cryptographic keys) and application programs (electronic cash, telebanking, symmetric encryption, and so on).

Certain smart cards also contain a cryptographic coprocessor that can handle asymmetric cryptographic algorithms, such as RSA.

Contactless Cards

In addition to these contact smart cards which require insertion into a reader device, there are also contactless cards available. These look just like a plastic credit card, but have a computer chip and an antenna coil inside, allowing it to communicate with a remote receiver or transmitter.

Contactless smart cards require only close proximity to an antenna in order to be read from or written to, and are thus ideal for applications where transactions must be processed quickly, as in mass-transit toll collection.

The development of contactless card technology was the catalyst for what are known as *"tags"*. Tags function like contactless smart cards but are in the form of a coin, a ring or even a baggage label. They are generally attached to objects such as gas bottles, cars or animals and can hold and protect information concerning that object. This allows the object to be managed by an information system – such as asset tracking or stock control - without any manual data handling.

Combination Cards

A hybrid of the two technologies is known as the combination card. This, as the name suggests, is a single card that is capable of functioning both as a contact and contactless card.

Virtual Smart Cards

The final category of smart card is something completely different, since it is software-based. With the "virtual smart card", the operation and data structure of a smart card is duplicated entirely in software. To an application requesting the presence of a smart card, however, the virtual kind appears exactly like a plastic one inserted in a card reader.

The virtual mart card has many of the same properties as a real one, but is simply a chunk of encrypted data stored on a user's hard drive or on a floppy disk. The user's PIN code, with a settable minimum length, is used as the encryption key for the data stored on the disk, so if the virtual smart card is stolen it will be harder to compromise. Virtual smart cards are a cheap, easy, and fast way to deploy smart card technology today, and to evolve into supporting real smart cards as they become more widely used.

The virtual smart card approach works very well for users that have mobile desktops or laptops, in that they travel and bring their complete system with them. On the other hand, real smart cards are a more effective solution for customers that have mobile users who do not carry anything with them other than just the card.

Although not as secure as a genuine smart card, the virtual smart card provides an ideal "half-way house" for remote or mobile users wishing to employ the highest levels of security available without having to use a hardware-based smart card reader.

A BRIEF HISTORY

Amazingly enough, smart cards are not that new an invention. They first appeared as long ago as 1974, created by Moreno/Innovation, although it was 1982 before the first serious trials took place in France. By 1985, French banks were convinced of the benefits of smart cards and began serious work on technology conversion, issuing 22 million of them to customers by 1993.

Smart cards are already considered "everyday" items in many European countries. Over 100 million pay phone cards and 22 million bank cards are in use in France; 80 million health insurance cards have been issued in Germany; more than 50 countries have implemented pay phone technology; and over 20 countries are using some form of "Electronic Wallet".

In the UK, the most common implementation of the full-size contact card technology at the time of writing is as a "viewing card" for satellite television services. A smart card containing customer information and subscription details must be inserted into the satellite receiver in order to enable viewing of encrypted transmissions.

SMART CARDS AND SECURITY

Since most smart cards are used for security-related applications, it makes sense that the design is such that physical access to the chip contents is prevented except under certain rigorously controlled conditions (such as when the correct PIN number is entered and verified).

Between them, the operating system and the functions of the user interface provide mechanisms for controlling access to data stored in the smart card.

Access to the information stored within a smart card can be tightly controlled in a number of ways, and separate access rights and conditions can be set for each application or set of stored data.

Who can access the information?

Basic smart card applications can be accessed with no security. The most obvious examples of this would be a library card or a medical records card, from which the patient's name and blood type can be read without need of a password.

Other applications – encryption or access to a telebanking system for example - may be accessed by the user of the card once a valid PIN number has been entered. Multiple unauthorized attempts to enter the PIN will result in the card being disabled.

The final category of application is accessible only to the third party who installed the application to the card - various payment applications, for instance, use smart cards as trusted devices. Not even the owner of the card can gain access to this category of application or data, a prime example of which is electronic cash, where the "wallet" can only be replenished by the issuing bank.

For applications of this nature in particular, it is apparent that smart card technology must be resistant to all forms of hacking or attempted unauthorized access. This would otherwise result in the equivalent of being able to print your own money, and thus needs to be guarded against if we are to rely on such technology to form the basis for a future cashless society.

How can the information be accessed?

Information on a smart card can be divided into several categories:

- *Read only*
- *Added only*
- *Updated only*
- *No access available*

Commercially sensitive data fields stored on a smart card – such as the amount of electronic cash available or the level of prepaid accounts – is usually only accessible by cryptographically secured commands. This prevents the holder of the smart card from manipulating these fields fraudulently.

This method, coupled with hierarchical key management on the card itself, can also be used to control the applications that can be loaded onto the smart card. A smart card issuer, for example, can control what data and applications are permitted on the card by securing the initial file structure with its own key.

Further personalization of the card is then subject to the authority of the issuer, who can determine if the user can alter the pre-loaded data, and whether or not the user is allowed to load his own data and applications.

WHY SMART CARDS?

Smart cards provide us with so much more in the way of security that has been hitherto available with software-only solutions. They provide an additional "physical" level of security over and above that offered by the usual password protection mechanisms.

For instance, if a password is compromised it is a simple matter for an unauthorized user to gain access to a protected system. When access to that system also requires the physical presence of a smart card in a reader (coupled with the entry of a PIN number to provide access to that card), life is made that much more difficult for the would-be hacker.

An additional benefit of smart cards is their ability to store a user's personal encryption keys and digital certificates. The fact that almost any number could be stored securely within a card means that we can issue a separate key per application per user if necessary. It also means we can use keys of the maximum length allowed by law in any given country, without having to rely on manual entry by the user.

Once the keys and certificates are safely stored within the card memory, they become completely portable. At the moment, a user's digital certificate is often locked to a particular application on a single machine – say a web browser on our machine at the office. This frequently necessitates obtaining multiple certificates for our browser at the office, at home and even on our laptop, which increases both the management burden and the potential security exposure. If the certificate could be stored within a smart card, however, and accessed by any application, then just one certificate is all that would be required.

It is even possible for the encryption process itself to be performed by the card, which is often far more secure than a PC. Several methods of attack are known against keys that are stored in computers such as PC's or workstations, or against cryptographic algorithms that are executed on a computer.

If we think back to our problem of multiple certificates and private keys installed on various machines, it becomes apparent that we can never physically secure all of these machines at the same time. It may thus be possible for a hacker to gain control of our office machine while we are out on the road, and gain access to the keys stored there.

Such attacks are impossible when using smart cards for storing the keys and performing the algorithm on the card. Keys can be stored on the card in such a way that they can be used by applications on the card but cannot be read in any other way. Since none of the really important information ever leaves the card an attacker who wants to use the key must have access to the smart card itself. Therefore unless the user is careless in leaving his card in a reader attached to the PC – and even then the use of the smart card is usually protected by a PIN number - unauthorized access becomes all but impossible.

Development Obstacles

Undoubtedly the biggest obstacle faced by the card industry so far is the general lack of standards. Proprietary solutions from all the major vendors to date have led to poor compatibility between applications, cards, and readers. The only initiative to date to achieve a standard is PKCS #11.

Having sourced the appropriate application the user is often severely restricted in his choice of card reader to work with it. Once the card reader has been selected, it is unlikely that cards from any other vendor will work with that reader. The lack of a standard model creates high development and maintenance costs and overall system administration complexity.

Some security software vendors – who obviously have an interest in seeing smart card technology flourish – have attempted to minimize the problems by creating drivers and card readers which are capable of working with a wide range of applications and cards. This is a good first step.

In the long term, however, what is required is a standard model for interfacing smart card readers to PC's, device-independent API's for application development, and resource sharing capabilities across multiple applications.

In order to promote interoperability among smart cards and readers, the International Standards Organization (ISO) developed the ISO 7816 standards for integrated circuit cards with contacts. These specifications focused on interoperability at the physical, electrical and data-link protocol levels.

In 1996, Europay, MasterCard, and VISA (EMV) defined an industry-specific smart card specification that adopted the ISO 7816 standards and defined some additional data types and encoding rules for use by the financial services industry. The European telecommunications industry also embraced the ISO 7816 standards for their GSM smart card specification to enable identification and authentication of mobile phone users.

While all of these specifications (ISO 7816, EMV, and GSM) were a step in the right direction, each was either too low-level or application-specific to gain broad inter-industry support. Application interoperability issues such as device-independent APIs, developer tools, and resource sharing were not addressed by any of these specifications.

PC/SC Workgroup

The PC/SC (Personal Computer/Smart Card) Workgroup was formed in May 1996 in partnership with major PC and smart card companies: Groupe Bull, Hewlett-Packard, Microsoft, Schlumberger, and Siemens Nixdorf. The main focus of the workgroup has been to develop specifications that solve the previously mentioned interoperability problems.

The PC/SC specifications are based on the ISO 7816 standards and are compatible with both the EMV and GSM industry-specific specifications. By virtue of the companies involved in the PC/SC Workgroup, there is broad industry support for the specifications and a strong desire to move them onto an independent standards tract in the future.

Since its founding and initial publication of the specifications in December 1996, additional members have joined the PC/SC Workgroup, including Gemplus, IBM, Sun Microsystems, Toshiba, and Verifone.

GENERAL APPLICATIONS

Smart cards are ideal as providers of tamper-resistant storage for protecting private keys, account numbers, passwords, and other forms of personal information. They also serve to isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a “need to know.”

In addition, smart cards provide a level of portability for securely moving private information between systems at work, home, or on the road. These factors combine to make smart card technology suitable for a wide range of applications for the general public.

Customer Loyalty Schemes

By simply using a smart card at the point of sale, stores are able to track customer preferences and buying patterns (targeted marketing applications) as well as allow customers to earn "points" towards services such as parking and meals at the store, or cash savings to be redeemed at the point of sale.

Although such schemes already exist using traditional magnetic stripe cards, the adoption of smart card technology provides increased security and flexibility. Several large retail outlets in Japan have already gone this way.

Travel & Transport

Airlines have begun implementing smart cards for ticket-less airline travel, boarding passes and receipts, as well as for the airlines' own version of the customer loyalty scheme, in the form of "air miles" or frequent flyer programs.

Other areas of the transport industry are using smart cards for electronic travelers checks, fare and toll collection, and even as car keys.

The government of Singapore, for instance, is proposing to implement a toll system that would communicate with cars and charge their smart cards as they pass various points on a road (as opposed to the simple vehicle identification systems already in use in the U.S. and elsewhere).

Electronic Banking

For many, electronic banking will be their first experience of financial transactions over the Internet. Whereas we all implicitly trust banks to keep our money safe on a day to day basis, there is nevertheless something worrying about performing monetary transactions over an open network such as the Internet.

Smart card technology can make this process incredibly safe. First, the client has to authenticate himself against the server before getting access to accounts, after which individual transactions have to be authenticated to prevent misuse or replay.

Without smart cards, the best protection that can be offered is the use of PIN numbers. Smart cards, however, provide a more secure means of authentication, coupled with the ability to encrypt all transactions within the card itself.

In the Financial markets, smart cards represent the next generation of credit and transaction cards. They are the future of electronic money and electronic commerce, and can be used for portfolio management and electronic signature verification, as well as secure banking access.

Multimedia & On-line Services

Many believe that the future of broadcast entertainment lies with video on demand and pay-per-view type viewing, and smart cards provide the ideal means to authenticate subscribers and remit payment in exchange for broadcast material.

Both customer and provider require a secure transaction system, since the provider does not want to supply material to non-subscribers, and customers need to be sure that they will only be charged for material they have viewed.

Another similar mechanism will eventually be required for on-line services offered over the Internet. As push technology catches on and bandwidth and reliability improves, on-line providers will inevitably begin charging for material that is subscribed to and specifically requested by users. Once again, the smart card provides the ideal means to authenticate subscribers, and to pay for material in terms of pages viewed or kilobytes downloaded.

Health Care

Health care applications include eligibility and payment verification where private medical insurance is in force, together with personal medical profiling and medical records stored on the smart card itself.

Home Use

Already in use in satellite TV decoders, the smart card reader will more than likely be integrated into the PC, personal Internet access appliance or set-top box, and even the television itself eventually.

In time, a single card and reader combination will provide access to subscription channels, pay-per-view events and the Internet, all driven from the comfort of your armchair.

Personal Records

Because of the security afforded by smart cards, they can be used to store drivers' licenses and car registrations, passport and official documents, medical records, electronic benefits, electronic voting, and electronic currency.

Telephones

This is the one area where people are already likely to encounter smart cards on a day to day basis.

Telephone cards can be "loaded" with units and used in public telephones. Similar to the electronic cash idea, they can be replenished once all units have been used. In France, the telecommunications authorities have already proposed general use of the smart cards now used at pay telephones.

An even more common usage is the SIM (Subscriber Identification Module). This is a miniature smart card consisting of just the chip on a plastic substrate, used by digital cellular (GSM) phone operators to enable the use of a GSM phone on their network.

Each SIM card contains a unique serial number to identify the customer to the GSM operator, and is protected by unlock codes and PIN numbers to prevent unauthorized usage should the phone or card be stolen. The card uses its EPROM memory area to store useful customer information such as frequently dialed numbers, phone settings (divert on busy or messaging options, for example) and SMS (Short Message Service) messages.

Unlike analogue cellular phones, it is the SIM card itself that defines the available service, and the phone is useless without it.

Internet Commerce

Although the Internet was originally designed more for the free exchange of information than as a base for secure financial transactions, many industry commentators feel that much of the future of the Internet lies with electronic commerce.

For the Internet shopper with a simple card reading device attached to, or even integrated in, his PC, the smart card is the ideal support for payment over the Internet, whether in cash or as credit.

Smart cards can provide the security you need to support e-commerce applications, with maximum security via strong authentication, secure storage of credentials, trusted implementation of algorithms and secure issuing of keys.

Electronic Cash

People are used to paying for goods and services using credit and debit cards these days, but are reluctant, or unable, to make small purchases using such payment methods.

Smart cards provide the means to implement true electronic cash solutions since their tamper-proof nature allows a financial institution to load them with a number of electronic “coins” or “notes”, or simply with an overall cash value, and for this value to be immune from user interference.

Purchases are made by inserting the card into a reader and keying in the amount, which is then transferred from the customer’s to the retailer’s card in a secure fashion. If large amounts of e-cash are to be carried within a card, transactions can be further protected by a PIN number. Retailers can upload their daily takings to the bank whenever convenient using modem connections or ATM machines.

In Denmark, a consortium of banking, utility and transport companies has already announced a card that would replace coins and small bills.

E-Cash and Privacy

Some people are worried about the lack of anonymity in such systems, however. Currently they are based on cards that identify themselves during every transaction (positive identification of the user is, of course, one of the benefits of smart cards), thus providing the capability to record each and every purchase made against your name for later analysis.

Cash, of course, has always offered complete privacy for the purchaser, an option that could be lost in a cashless society if we are not careful. Personal privacy could be seriously eroded, with law enforcement officers (or criminals!) able track your every move without leaving their PC – the ultimate Orwellian nightmare for some.

Payment systems have been developed that are untraceable and anonymous, however. In such systems, e-cash is implemented in the form of digital signatures called *"coins"* that represent a certain fixed amount of money, but which are not "tied" to individual users.

A bank issues these coins to the user and charges them to their conventional account. Each coin can be used only once, and the receiver must send them directly to the digital bank, whereupon the bank merely verifies that the coins are valid and that they have not been previously spent. There is no "audit trail" leading back to the purchaser.

Where personal information is stored on a smart card, it should be under the control of the holder just how much of that information is released or made available to host applications. In general terms, the choice between keeping information in the hands of organizations or of individuals is being made each time any government or business decides to automate another set of transactions. In one direction lies the potentially unwelcome scrutiny and control of people's lives, in the other, a more balanced approach between privacy and the needs of the financial community and authorities.

Smart cards have the potential to simplify our daily lives, yet they are also open to abuse by authority. Allowing users to retain control of their personal information does not impact on the effectiveness of the technology, whereas the knowledge that each and every transaction could be logged and used against you may well have a negative effect on its uptake.

The shape of society in the next century may well depend on which approach predominates.

ENTERPRISE SECURITY APPLICATIONS

In addition to those general-purpose applications already mentioned, smart cards also have a niche to carve in the work place.

They are capable of enhancing software-only solutions such as client authentication, single sign-on, secure storage, and system administration, making them suitable for both physical and logical access control applications in the enterprise.

By personalizing the smart card with the holder's name and photograph, it can act both as a general purpose employee ID card (for visual recognition) and an access control mechanism.

Physical Access Control

The simplest concept of access control is the restriction of the general public from entering business premises, which can obviously be accomplished by locking the doors.

Employees need access to their workplace, however, so locking the doors is not practical during working hours. A very simple solution could be to install "cipher" locks on door locks that have push-button key codes. These have a couple of serious disadvantages, however.

The first is that the code needs to be kept fairly short and cannot be changed too regularly, otherwise it will cause difficulty with genuine staff forgetting the access code. The second is that it is not too difficult for an outsider to watch over the shoulder of a member of staff while the code is being entered. That person would then have access to the premises until the next code change.

Card Readers

A more secure method of access control is to use individually coded smart cards for employees and visitors, together with card readers placed at entry doors, parking lot entrances, and internal locations where access needs to be controlled. The door is held shut either by an electric door strike or a magnetic shear lock, and can only be released under control of the card reader (or following power loss).

For speed and ease of use, contactless or combination cards would be chosen for such applications in order to facilitate rapid movement through the premises. When an employee or visitor passes a badge near a reader, the door will unlock automatically if the person is authorized to enter.

PIN Numbers

Where a higher level of security is required, however, you may wish to augment the use of a smart card with a PIN entered via an ATM-type key pad. In such cases, where physical contact is required anyway, lower-cost contact smart cards would be quite acceptable.

Access to particular areas can be easily controlled via a computer system. It can limit access to certain employees during certain hours, and would facilitate rapid change of access permissions during vacations and holidays. Visitors can also be issued badges that only allow access to certain areas on the day of the visit.

Big Brother Is Watching You!

Records of entry and exit times for each person can be kept for a comprehensive audit trail, use in time and attendance systems, or for billing, such as in parking areas.

Systems can determine if a specific person is in the building – perhaps pinpointing him to an actual room - so messages or calls can be relayed to him.

Reports can also be generated that list all activity at a specific location, during a period of time, or even the activity of a certain person

Biometrics & Booths

For high-risk applications, you may need to install *biometric readers* or *Personal Identity Verification* (PIV) devices. The most commonly used today are hand geometry, eye retina scans, finger identity and voice recognition.

These could be coupled with a secure booth or two-door configuration in order to prevent "tailgating" (where an unauthorized person quickly follows an authorized one through an open door).

In a booth application, a card reader and keypad configuration gives access to the first door, and the second door will not open until the first is closed and locked. In high-security areas, a weight pad measures the person's weight to ensure only one person is in the booth at a time, and a PIV device is used in the booth to verify the person entering. Once the employee identity is verified in the booth, the second door opens permitting access to the secure area.

Although some of these applications sound a little extreme, they are in regular use today in many military, scientific and even some medical establishments throughout the world.

Logical Access Control

Once an employee has gained access to the building and settled at his desk, the next task is to log on to the network.

Local Network Access

With a smart card reader attached to the PC, the same card that provided access to the building can provide the first line of authorization for the network.

In identifying himself to the smart card (via PIN number or password) the card itself would then contain the necessary digital certificates and passwords to authenticate the user to all the appropriate network resources.

Fine-grained control is provided for the network administrator, who is free to allocate numerous different passwords for each user according to the applications required, and those passwords could be almost any length.

This would make life extremely difficult for anyone attempting to gain access to the network resources without a smart card, whilst still providing a single sign-on for the authorized user.

Client-Server Applications

Traditional network single sign-on requires that all network and application passwords are identical for each user, thus requiring the user only remember the one password.

Using smart cards, however, client-server applications could be covered by two (or even more for three-tier applications) levels of password protection.

The first challenge comes at the client level, when the user first logs onto the network and fires up the application. The second challenge comes as the client software attempts to connect to the back-end server. This is all transparent to the end user who still only has to authenticate himself once to the smart card.

In the background, settings on the card itself mesh with those set on the network to determine exactly what applications are available to the holder of the card, with passwords being supplied automatically whenever necessary.

Virtual Private Networks

Virtual Private Networks (VPN) provide a transparent encrypted link between two sites across the Internet. The link appears as a simple point to point connection, thus allowing existing applications to use it without modification. This provides the equivalent of a global private network without the complication or expense of installing dedicated communications links.

VPN's are usually controlled by firewalls at each of the sites to be linked, with all data travelling between those sites encrypted whilst in transit.

Use of the VPN link is controlled by the firewall, and smart card-based authentication would provide an additional tamper-proof level of access control for clients wishing to use the VPN.

Remote Access

A new trend in the work place is "teleworking", where an employee works from home or some other remote location (such as a hotel room) using a laptop or PC that is connected to the corporate network either directly or via the Internet.

Remote access of this nature poses a significant security threat to the company's network, and demands new facilities from network security systems which "traditional" firewalls cannot address.

One such problem area is security for external interaction with business systems on the internal network – a vital requirement for effective remote access. While the standard firewall architecture provides an effective solution to the problem of unauthorized access, it can frequently hinder the use of the Internet for anything other than basic functions such as Web browsing or simple e-mail.

Many users are beginning to come up against the limitations of traditional firewalls, making it difficult to expand the usage of the Internet into other areas of the organization. The problem is that they were originally built as one-way devices, designed to block all incoming connections and effectively keep people out. With the growth in remote working, however, it is increasingly important to allow effective two-way conversations to occur between two authorized parties through an otherwise secure firewall.

The issue now becomes how to provide a secure, fine-grained access-control and encryption channel between specific users and applications *outside* the firewall and the corporate application software *behind* the firewall. This needs to happen in order to support client-server applications across the Internet, but it needs to happen in such a way that allowing remote users to communicate with a protected network via the firewall does not at the same time open a channel which potentially could be exploited by unauthorized users.

When linking two sites together across the Internet, we can make use of the VPN feature mentioned in the previous section. The drawback is that it requires a firewall at each end, and is thus only of use when connecting sites or organizations. Effective remote access requires that we provide a temporary link between the remote employee and the corporate network which is equally secure, yet is created and removed dynamically.

This can be achieved using special client and server-side software that works with the firewall to provide such dynamic links. This is secured using smart card technology, which can perform all necessary key storage, authentication and encryption on board the card itself.

One of the biggest advantages of using smart card technology is that during the initial mutual authentication phase when the client and server are creating the secure link, the client key never actually leaves the smart card. Instead, all the necessary responses are calculated and encrypted within the card and then transmitted directly to the server software.

This not only provides us with the means to support remote access for employees, but also the means to offer a client-server link into selected resources on our internal network for users outside our organization, perhaps to support Internet commerce applications.

This can be achieved via the use of server-side software capable of managing subscriber enrolment, followed by the secure distribution of either a real or virtual smart card.

Data Encryption

Encryption is all about transforming plain text into a form unreadable by anyone without a secret decryption key. It thus allows secure communication over a general purpose insecure channel, such as the Internet.

Although the mathematics behind it can be very complex, encryption itself is pretty straightforward. Cast your minds back to when you were kids and you wanted to send secret messages to each other. The simplest form of encryption was the one where every letter of the alphabet was substituted for the one "*n*" positions following it.

Here we are introduced fairly painlessly to the two most important buzzwords in the cryptography world: the "*key*" is the number of positions we are shifting the letters, whilst the "*algorithm*" is simply the idea that the encrypted letter is the one "*n*" places following the plain text letter.

There are two ways you can beef up security on this – increase the length of the key, and devise ever more complex algorithms. Luckily, we do not have to get involved in creating our own algorithms, since there are some perfectly acceptable standards out there, the main ones being DES (Data Encryption Standard), triple DES, IDEA (International Data Encryption Algorithm) and RC4.

Whereas the original DES algorithm uses 56 bit keys, later and more powerful systems use much longer ones, forcing potential hackers to run through trillions of combinations in any attempt to find the right one by brute force.

Triple DES is an enhanced version of the original DES algorithm and encrypts data three times using three different keys (providing an effective key length of 112 bits). IDEA is a 128 bit mechanism developed by the University of Zurich in 1992 and is a favorite of European financial institutions.

Smart cards can be used to store both the keys and the algorithms themselves, with some cards even incorporating a dedicated encryption processor.

The smart card can also control how and when data is encrypted. At the basic level, for instance, perhaps all data travelling out of the organization via e-mail is automatically encrypted. For certain users, however, it may also be prudent to encrypt all data written to the hard disk at file level too, automatically decrypting it on the fly whenever it is accessed (providing the smart card used to encrypt it is present).

THE FUTURE

From this point onwards, we are likely to see the introduction of PC's and Network Computers with integrated smart card readers. These can be implemented either as part of the keyboard or occupying one of the 3.5 inch drive bays, or perhaps as external units or PCMCIA devices.

Predictions for future growth include a 40 per cent increase in Europe, a 25 per cent increase in Asia, a 15 per cent increase in the US and Canada, and an 8 per cent increase in South America. Total predictions of growth cite 4 billion units by the year 2000 (*Source: Hewlett Packard*).

As we have already mentioned, the "smartness" of smart cards comes from the integrated circuit embedded in the plastic card. Yet the physical appearance of the smart card is driven mainly by the need for familiarity and convenience of handling – so the credit card size and shape is an obvious one.

That same electronic function could be performed by embedding similar contactless circuits in other everyday objects, however, such as key rings, watches, badges, glasses, rings or earrings.

The use of biometrics within the card itself will mean that a person can be reliably identified by his or her hand, fingerprints, retina of the eye or sound of the voice. Soon it will be possible to authorize the use of electronic information in smart cards using a spoken word or the touch of a hand.

SUMMARY

Modern society needs an enormous amount of information in order to function effectively. Computers give us the means to process this information, and smart cards give us a way of individualizing its handling and control – both at home and in the work place.

Although a relatively new technology, the smart card already affects the everyday lives of millions of people. This is just the beginning and will ultimately influence the way that we work, shop, see the doctor, use the telephone and enjoy our leisure activities.

In order to move on from this point, however, and drive the uptake of smart card technology, we need wider implementation of standards in order to allow universal writing and reading of the cards.

In the short term, some vendors are working hard to provide readers that can handle cards from multiple vendors, and drivers that can sit between applications and card readers from multiple vendors. This at least allows users to begin implementing smart card applications safe in the knowledge that they can mix and match components to a certain extent.

However, in the long term, smart vendors will comply with upcoming standards to ensure widespread acceptance. Only when we have a universal standard can we begin to realize the dream of a single card for all our personal and work-related data.