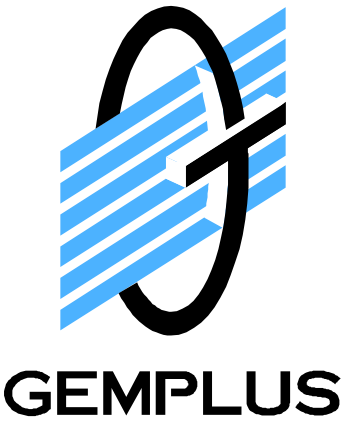


GemSAFE

White Paper

Understanding the fundamentals of smart card enabled security for Web and E-mail

&

Setting up GemSAFE Applications

CONTENTS

1. The need for smart card in Web and E-mail

A smart card = data storage + data processing in a plastic body!

Any PC has more memory capacity and has more processing power than a smart card. So why use a smart card in this environment?

Using smart cards in IT systems is a fairly recent concept, but now widely accepted by the IT world. Smart cards have been adopted because they bring unmatched security. Today, the vast majority of IT world players have designed their products to incorporate smart card technology. The IT industry has defined standards to allow smart card integration into open architectures. Before going into the technical side of this integration, let's have a look at the various benefits of smart card solutions (because security is only one facet of the smart card.) compared to software-only solutions.

1.1 Security

This is inherent in smart cards. Smart cards are designed to ensure the highest security levels, because they are used to give access to valuable services: phone, pay-TV, credit transactions, cash, etc. From silicon design and manufacturing to card operating system qualification, everything in a smart card has security as a primary target. Gemplus production and R&D for instance are subject to stringent audits from financial institutions to control each step of the process. Microprocessor and associated memories include security mechanisms to lock itself in case of physical, electrical, chemical attacks. These examples among others clearly demonstrate that a smart card cannot be compared to a PC.

There is therefore no better place to store your private keys that will be used to prove your identity to a Web server or sign an E-mail or decrypt an E-mail. Where else could credentials be more secure?

1.2 Mobility

More and more users connect from various Internet devices. PCs at work and at home, a kiosk at the airport, and it's just the beginning. Webphones, mobile phones, TV settop boxes: many Internet appliances are making Internet access pervasive. So why would an individual want to be tied to a single PC architecture? The smart card IS the individual on the Net. Light, attractive looking, in a reliable consumer package, it fits in every wallet and you always have your electronic ID with you.

1.3 Simplicity

Plug your smart card in, you get access to your personal Web services and your E-mail box. Remove it, nobody else will be able to do this, or sign or decrypt an E-mail on your behalf. Can you imagine a simpler way to protect your digital assets?

2. GemSAFE overview

GemSAFE is a smart card-based turnkey solution for securing the access to Web sites as well as the exchange of E-mails. With the Internet marketplace, companies can offer on-line services to a larger audience at a reduced cost. These services range from e-commerce, home-banking, to e-citizen, home-training and E-mail. Web perspectives are huge, but the lack of security prevents them from really happening. Gemplus breaks down this major barrier with GemSAFE, a reliable plug-and-play smart card solution that secures your transactions on the Net.

GemSAFE is a secure and portable electronic passport for accessing Web applications and popular E-mail systems through Microsoft and Netscape browsers. The smart card stores your secret information and thus prevents anyone from stealing your identity. It is as simple as inserting your personal card in a slot!

2.1 Both open and secure

The latest standards like SSL3/TLS (Web access) or S/MIME (E-mail) allow inter-operability for security services between any browser interface and any Web server. However, security hole of these protocols is the management of your personal keys and certificate that can easily be tampered on your PC. Having a very secure padlock is of no use if it's easy to steal your keys! GemSAFE integrates seamlessly with these protocols but offers the highest level of security for storing your credentials. The smart card solution allows a secure storage, but also performs cryptographic algorithms, so that your keys never leave the card. Achieving this level of security brings an unmatched opportunity to leverage your IT investments by exploiting the most sensitive services over the Net. Just plug your smart card in. Many Banks, Telcos, Pay-TV operators are relying every day on million of smart cards to perform billions of transactions!

2.2 Always in your pocket

With the GemSAFE solution, a user is no longer dependant on his local computer. Travelling with his electronic identity in his pocket, he can access securely his on-line services with his personal smart card, protected by a pin-code, from any machine in the world.

3. Industry standards

3.1 PKI introduction

The RSA Public Key Cryptosystem was discovered in 1977 by Ronald Rivest, Adi Shamir, and Len Adleman, then professors at the Massachusetts Institute of Technology.

Rather than using the same key to both encrypt and decrypt data, the RSA system uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation upon the data. Each key is the inverse function of the other; what one key does, only the other can undo.

The RSA Public Key is made publicly available by its owner, while the RSA Private Key is kept secret. To send a private message, an author scrambles the message with the intended recipient's Public Key. Once so encrypted, the message can only be decoded with the recipient's Private Key.

Inversely, the user can also scramble data using their Private Key; in other words, RSA keys work in either direction. This provides the basis for the "digital signature," for if a message can be unscrambled with with a user's Public Key, the user must have used his or her Private Key to scramble it in the first place. Since only the owner can utilize their own private key, the scrambled message becomes a kind of electronic signature -- a document that only the user can produce but everybody who has a copy of his RSA Public Key can verify.

3.2 Digital signature : Authentication & Nonrepudiation

A digital signature is created by running message text through a hashing algorithm. This yields a message digest that is effectively a very condensed version of the original text (a good hash function has the property that it is practically not possible to find two messages that compute to the same message digest). The message digest is then encrypted using the private key of the individual who is sending the message, turning it into a digital signature. The digital signature can only be decrypted by using the public key of the same individual. The recipient of the message decrypts the digital signature and then compares this with an a message digest recalculated from the original message text. If the two match, the message has not been tampered with. Since the public key of the sender was used to verify the signature, the text must have been signed with the private key known only by the sender. This entire authentication process is incorporated naturally into a security-aware application.

3.3 What is a Digital certificate?

Users of RSA technology typically attach their unique Public Key to an outgoing document, so the recipient need not look up that Public Key in a public key repository. How can the recipient be assured that this Public Key, or even one in a public directory, really belongs to the person indicated? Could an intruder not masquerade in the computer network as a legitimate user, literally sitting back and watching as others unwittingly send sensitive and secret documents to a false account created by the intruder? The solution is the Digital certificate -- a kind of **digital "passport".** The Digital certificate is the user's Public Key that has itself been "digitally signed" by someone trusted to do so. The following figure presents a pictorial description of a Digital certificate.

Every time someone sends a message, they attach both their digital signature *and their Digital certificate*. The recipient of the message first uses the Digital certificate to verify that the author's Public Key is authentic, then uses that Public Key to verify the message itself. This way, only one Public Key, that of the certifying authority, has to be centrally stored or widely publicized, since then everyone else can simply transmit their Public Key and valid Digital certificate with their messages.

Using Digital certificates, an authentication chain can be established that corresponds to an organizational hierarchy, allowing for convenient Public Key registration and certification in a distributed environment.

3.4 Certification Hierarchies

Once a user has a Digital certificate, what do they do with it? Digital certificates have a wide variety of uses ranging from inter-office electronic mail to global Electronic Funds Transfer (EFT). In order to use Digital certificates there must be a high degree of trust associated with the binding of a Digital certificate to the user or organization linked with the Digital certificate. This trust is achieved by building hierarchies of Digital certificates, with all members of this hierarchy adhering to the same set of policies. Digital certificates will only be issued to people or entities, as potential members of a hierarchy, once proof of identity has been established. Different hierarchies may have different policies as to how identity is established and how Digital certificates are issued.

3.5 What is X.509 certificate?

ITU-T Recommendation X.509 specifies the authentication service for X.500 directories, as well as the widely adopted X.509 certificate syntax. The initial version of X.509 was published in 1988, version 2 was published in 1993, and version 3 was proposed in 1994 and considered for approval in 1995. Version 3 addresses some of the security concerns and limited flexibility that were issues in versions 1 and 2.
Directory authentication in X.509 can be carried out using either secret-key techniques or public-key techniques; the latter is based on public-key certificates. The standard does not specify a particular cryptographic algorithm, although an informative annex of the standard describes the RSA algorithm.

An X.509 certificate consists of the following fields:

- version
- serial number
- signature algorithm ID
- issuer name
- validity period
- subject (user) name
- subject public key information
- issuer unique identifier (version 2 and 3 only)
- subject unique identifier (version 2 and 3 only)
- extensions (version 3 only)
- signature on the above fields

This certificate is signed by the issuer to authenticate the binding between the subject (user's) name and the user's public key. The major difference between versions 2 and 3 is the addition of the extensions field. This field grants more flexibility as it can convey additional information beyond just the key and name binding. Standard extensions include subject and issuer attributes, certification policy information, and key usage restrictions, among others.

X.509 also defines a syntax for Certificate Revocation Lists (CRLs).

The X.509 standard is supported by most cryptographic standards, including PEM, PKCS, S-HTTP, S/MIME and SSL.

3.6 How do I use Digital certificates?

Many applications, such as secure Web browsers and S/MIME-compliant E-mail tools, support the use of Digital certificates for electronic communications. In a Web browser, once your Digital certificate with a corresponding private key is installed, the browser uses it automatically when you access sites that request a Digital certificate. Sites can then use your digital certificate (coupled with your digital signature of a random challenge phrase generated dynamically by the server) to determine what information or services to allow you to access.

For example, a site could check your digital certificate against a list of paying members, recognize that you have paid for access to live stock quotes, and allow you to access up to the minute stock prices. You do not have to enter a member name, number, or password--your digital certificate is used to verify your identity automatically. You do not have to remember a different membership ID and password for each service you access, and the services are assured that someone else isn't accessing the information using your account.

3.7 Why Smart Cards?

Private keys must be stored securely, since forgery and loss of privacy could result from compromise. The measures taken to protect the private key must be at least equal to the security of the messages encrypted with the key. The private key should never be stored anywhere in plain text form. The simplest storage mechanism is to encrypt the private key under a password and store the result.

But storing the encrypted key on a disk, a floppy disk or a local hard disk, doesn't thwart attacks.

It might be best to store the key and the digital certificate in a smart card protected by a pin code.

The smart card is :

- unique and can't be cloned
- pin protected
- not accessible to other users
- a removable media that the user can remove and take with him when he finishes using a particular computer
- a secure portable safe for the user's sensitive data

3.8 Secure E-mail - industry standards and trends

The need for secure E-mail, in terms of both:

- authentication of the sender, and

- end to end (or user-to-user) privacy

has long been identified as critical to the growth of the on-line community. However, early standards such as PEM (Privacy Enhanced Mail) and MOSS failed to capture the industry's imagination.

Secure/Multipurpose Internet Mail Extensions (S/MIME), an initiative driven by RSA Data Security Inc., is currently an IETF Internet Draft. S/MIME was designed to add security to E-mail messages in standard MIME format with an emphasis on global inter-operability. Many key industry players are part of this initiative including both Microsoft and Netscape and many other E-mail application suppliers. The latest version of both the Netscape and the Microsoft Browsers are bundled with an S/MIME compliant E-mail application. Importantly, both of these products allow the most sensitive security tasks, such as digital signature or decryption of in-coming E-mails, to be sub-contracted to an external module such as a smart card.

Pretty Good Privacy (PGP) currently the only real competitor of S/MIME for a secure E-mail standard is both a specification and an application. It already has a large internet user base but in its original form, its Web-like trust model is not particularly well suited for scaleability. In response to the S/MIME initiative, a version known as OpenPGP has been proposed as an IETF Internet Draft that overcomes most of these limitations. OpenPGP currently receives less industry support than S/MIME and, considering the investment many key companies are making in S/MIME, this is unlikely to change in the near future.

3.9 Secure Web sessions - industry standards and trends

Securing an on-line session between a server and client for applications such as Web(HTTP), News(NNTP), File Transfer(FTP), Mail (SMTP), Distributed objects (CORBA), etc. may require:

- Dynamic authentication of the client by the server at the beginning of the session
- Dynamic authentication of the server by the client at the beginning of the session
- Privacy and proof of origin(integrity) for the data exchanged

Netscape proposed a protocol in 1993 known as SSL version 2 (Secure Socket Layer) which aimed to provide these services at a level between TCP/IP and the application layer (HTTP, FTP, etc.). This protocol was subsequently was improved to become SSLv3.0. Key features of this protocol are that the type of cryptographic services and algorithms (including key lengths) are negotiated between server and client as part of the protocol.

Most products (including the Microsoft browser and Microsoft servers) now support SSLv3. The SSL standard's dominant position is being confirmed as it has become (with very minor changes) an IETF Internet Draft known as Transport Layer Security (TLSv1.0). SSL/TLS is very widely implemented particularly in conjunction with HTTP which is known as HTTPS (not to be confused with sHTTP which is an early " Web only " security protocol). HTTPS can be found in almost all browsers and server software.

The only real competitor in the near future to the SSL/TLS initiative might be IPv6 (or IPng as it is also known as). IPv6 is the next generation of the packet level internet protocol and includes cryptographic services such as authentication and privacy at this level. However, the significant limit to the rapid uptake of IPv6 is the considerable investment that has been made world-wide in devices that support the current IP protocol version.

3.10 PKCS#11(Cryptoki) architecture as used by Netscape Browsers

Public Key Cryptographic Standard #11 Cryptographic Token Interface also known as Cryptoki is a standard that is maintained and published by RSA Data Security Inc. with the help of wide industry consultation. It is the only widely supported low level platform independent standard for interfacing with cryptographic devices.

The standard describes a normalised interface (in the C programming language) for accessing cryptographic engines. These engines are known as tokens. A token is capable of storing sensitive and non-sensitive data, managing access rights and, most importantly performing cryptographic calculations. All this functionality is available via the Cryptoki interface. In addition, an application can interrogate the token via the Cryptoki interface to find out his capabilities - so not all tokens have to provide the same level of functionality.

The implementation behind the interface is not defined in the standard. The algorithms and data storage functions could be implemented in software, in hardware (smart card, " black box ", PCMCIA card, etc.) or a mixture of both. There is a steadily increasing number of cryptographic device manufacturers which provide a PKCS#11(Cryptoki) interface for accessing their device. Equally there are an increasing number of application providers who rely on a PKCS#11(Cryptoki) module for their cryptographic needs. Not least among these is Netscape Communications Corp., who are transferring all their servers and browsers to this architecture. The latest version of their browser (Communicator 4.0) relies totally on internal or external modules which provide a PKCS#11(Cryptoki) interface to provide security services such as SSL and S/MIME.

The Netscape approach is fairly flexible. The browser interrogates installed external modules to find out what they can do. Anything that they are not capable of is subcontracted directly to an internal Netscape (software) PKCS#11(Cryptoki) module.

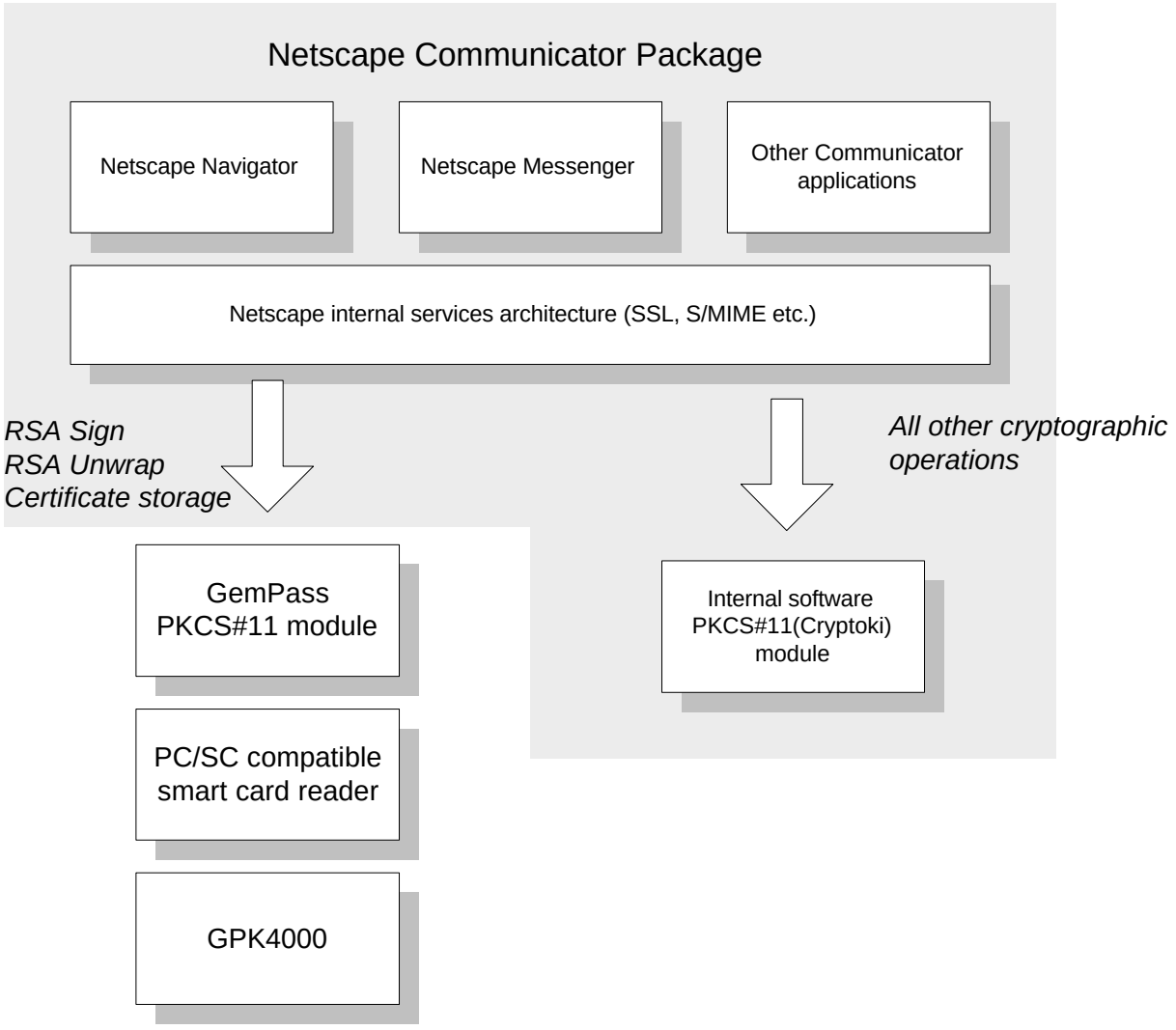
For the GemSAFE product, an external module with a PKCS#11(Cryptoki) interface is installed which uses the GPK4000 smart card as a cryptographic engine/data storage. Operations carried out by the card are:

- Signature using the RSA private key that is securely (utilisation is pin protected, read is never possible) stored in the GPK4000 smart card. This is used for client authentication in SSL and signing outgoing E-mails in S/MIME.

- Unwrap (decryption of the session key) using the RSA private key securely stored in the card (for decrypting incoming E-mails in S/MIME). However, the bulk decryption of the entire body of the message using the session key is carried out in the Netscape (software) internal module.

- Storage of user certificate(s)

All other cryptographic operations necessary (including all symmetric key operations) are subcontracted by the browser to the Netscape internal PKCS#11(Cryptoki) module. This is shown in the diagram below.



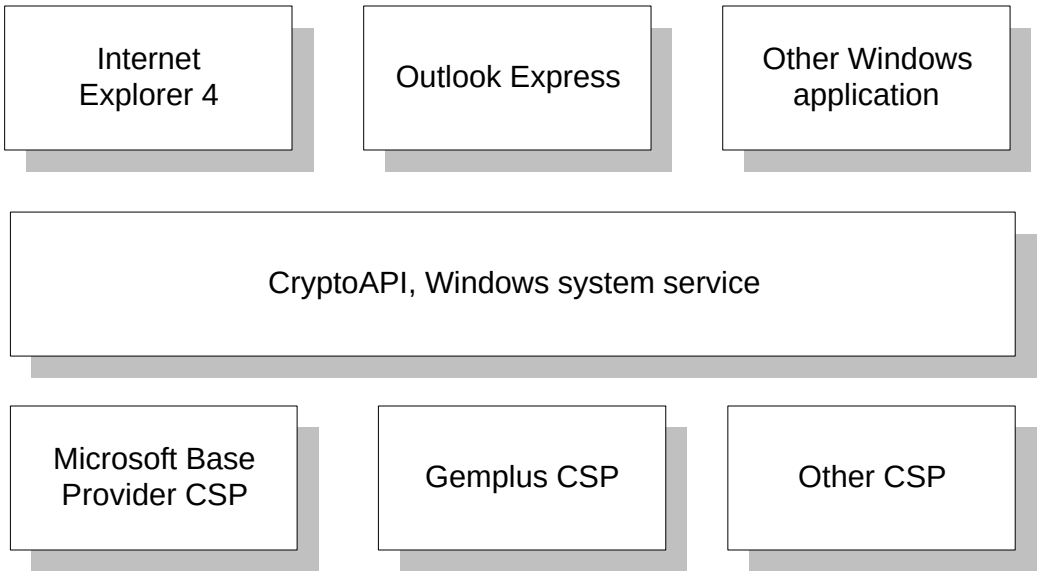
Note that the maximum symmetric key length allowed is determined by two things:

- The maximum length of the session key that the GPK4000 is allowed to unwrap.

- The symmetric key capabilities of the internal Netscape PKCS#11(Cryptoki) module. Generally the US version of the product provides up to 128 bit key lengths whereas the international version is limited to 40 bits.

3.11 Microsoft CSP architecture as used by Microsoft Browsers

Microsoft provide a cryptographic service architecture for their Windows operating system as shown below.



Thus any applications requiring a cryptographic service asks the system service " CryptoAPI " to provide it. This system service will allow the application to communicate with any installed cryptographic device drivers (known as Cryptographic Service Providers(CSP)). A software CSP known as the " Microsoft Base Provider " is always present and exists in two versions; US and international. The international version having more severe (40 bit) limitations on symmetric key lengths.

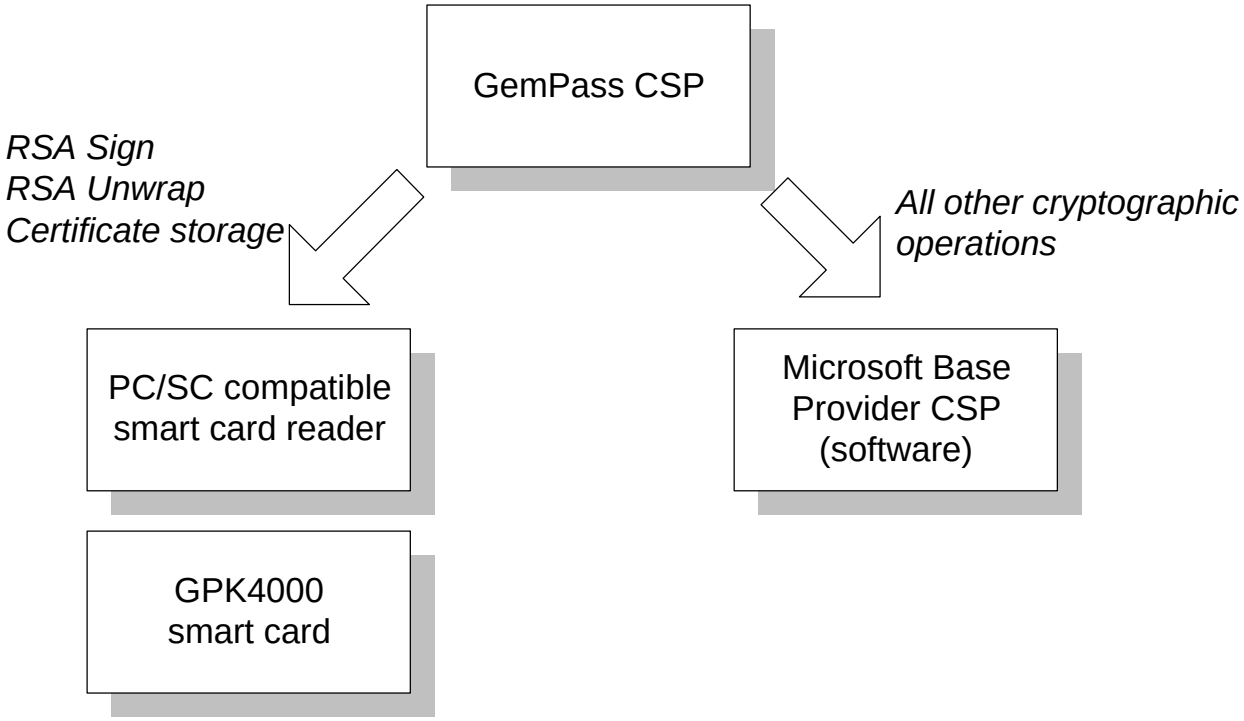
CSPs themselves have a type to indicate their capabilities. Applications such as the Microsoft browser Internet Explorer 4.0 and the Microsoft E-mail application Outlook Express require a fully functional " RSA_BASE " type of CSP to provide SSL and S/MIME services.

The GemSAFE solution is to provide a CSP that subcontracts sensitive cryptographic operations to the GPK4000 smart card and less sensitive operations to the Microsoft Base Provider. Operations carried out by the smart card are exactly the same as in the Netscape solution:

- Signature using the RSA private key that is securely (utilisation is pin protected, read is never possible) stored in the GPK4000 smart card. This is used for client authentication in SSL and signing outgoing E-mails in S/MIME.

- Unwrap (decryption of the session key) using the RSA private key securely stored in the card (for decrypting incoming E-mails in S/MIME). However, the bulk decryption of the entire body of the message using the session key is carried out in the Netscape (software) internal module.

- Storage of user certificate(s)



Note that the maximum symmetric key length allowed is determined by two things:

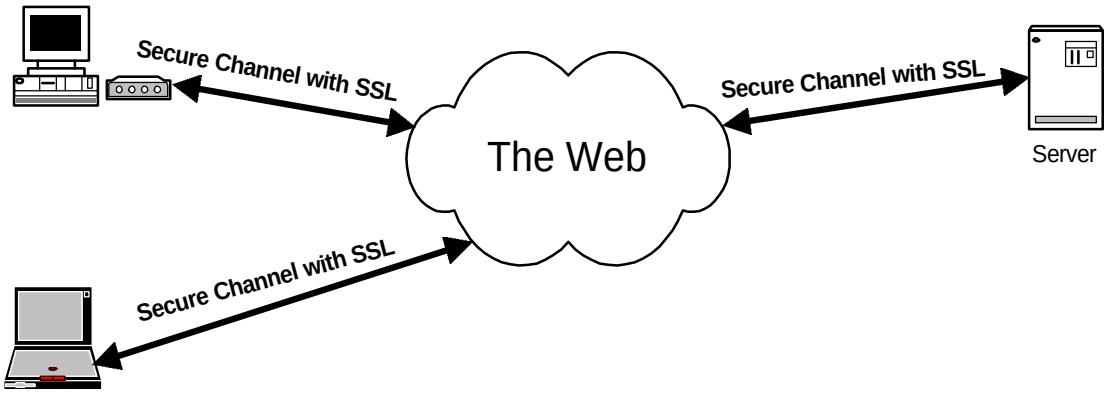
- The maximum length of the session key that the GPK4000 is allowed to unwrap. The US version of this smart card imposes no limits whereas the international version is limited to 40 bits.

- The symmetric key capabilities of the RSA Base Provider CSP. Generally the US version of the product provides up to 128 bit key lengths whereas the international version is limited to 40 bits.

3.12 Understanding SSL/TLS

The Secure Sockets Layer protocol is a security protocol that provides privacy over the internet. The protocol allows client/server applications to communicate in a way that cannot be eavesdropped. A " higher level " application protocol like HTTP can layer on top of the SSL/TLS protocol transparently.

The SSL protocol provides **" channel security "** which has three fundamental security services, all of which use **public-key techniques**.



SSL offers the following basic features:

- **Data privacy**
- **Data integrity**
- **Mutual authentication**

3.12.1 Message privacy

Data privacy is achieved through a combination of public-key and symmetric key encryption, as described above. All traffic between an SSL server and SSL client is encrypted using a key and an encryption algorithm negotiated during the SSL handshake. Encryption thwarts eavesdroppers who can capture a TCP/IP session using devices such as IP packet sniffers. Even though packet sniffers can still capture the traffic between a server and client, the encryption makes it impractical for them to actually read the message.

3.12.2 Data integrity

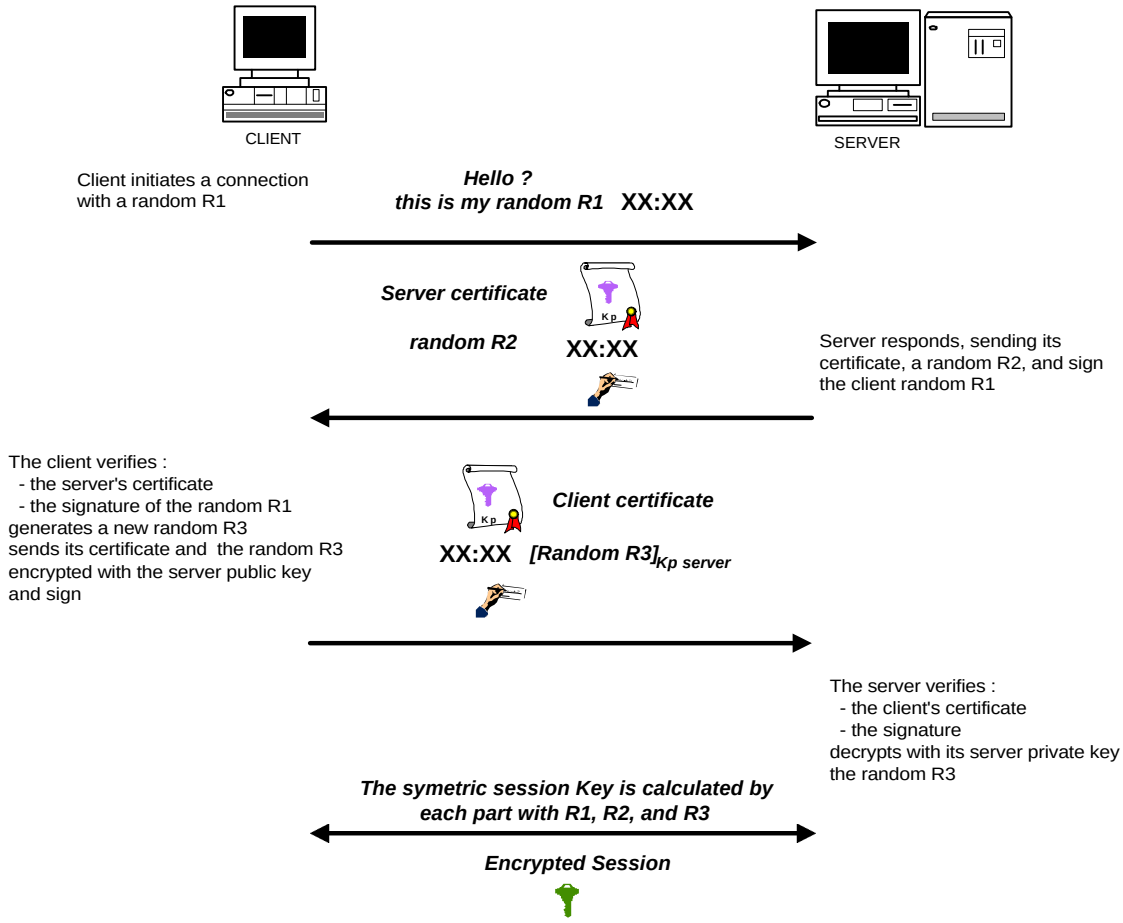
The data integrity service ensures that SSL session traffic does not change en route to its final destination. If the Internet is going to be a viable platform for electronic commerce, we must ensure that vandals do not tamper with message contents as they travel between clients and servers. SSL uses a combination of a shared secret and special mathematical functions called hash functions to provide the message integrity service.

3.12.3 Mutual authentication

Mutual authentication is the process whereby the server convinces the client of its identity and (optionally) the client convinces the server of its identity. These identities are coded in the form of public-key certificates (X.509), and the certificates are exchanged during the SSL handshake.

To demonstrate that the entity presenting the certificate is the legitimate certificate owner (rather than some impostor), SSL requires that the certificate presenter to digitally sign the data exchanged during the handshaking. The exchanged handshaking data includes the entire certificate. The entities sign the protocol data (which includes their certificates) to prove they are the legitimate owner of the certificate. This prevents someone from masquerading as you by presenting your certificate. The certificate itself does not authenticate; the combination of the certificate and the correct private key does.

3.12.4 Authentication and encryption process example



3.13 Understanding S/MIME

S/MIME is a new standard for encrypted and digitally signed electronic mail. Developed by RSA, S/MIME enables users of Web messaging clients such as Netscape Messenger or Outlook Express to send encrypted messages and authenticate received messages. S/MIME delivers message encryption and authentication with the flexibility, inter-operability, and cost-effectiveness of Web-based messaging.

S/MIME offers users the following basic features :

- Encryption for message privacy
- Sender authentication with digital signatures
- Tamper detection
- Interoperability with other S/MIME-compliant software

3.13.1 Private messaging

S/MIME's encryption helps ensure that your messages remain private. Netscape Messenger and Outlook Express software support domestic and export-level public key and symmetric key encryption.

3.13.2 Sender authentication

S/MIME authenticates the message sender by reading the sender's digital signature (the recipient can see who signed the message and view the certificate for additional detail).

3.13.3 Tamper detection

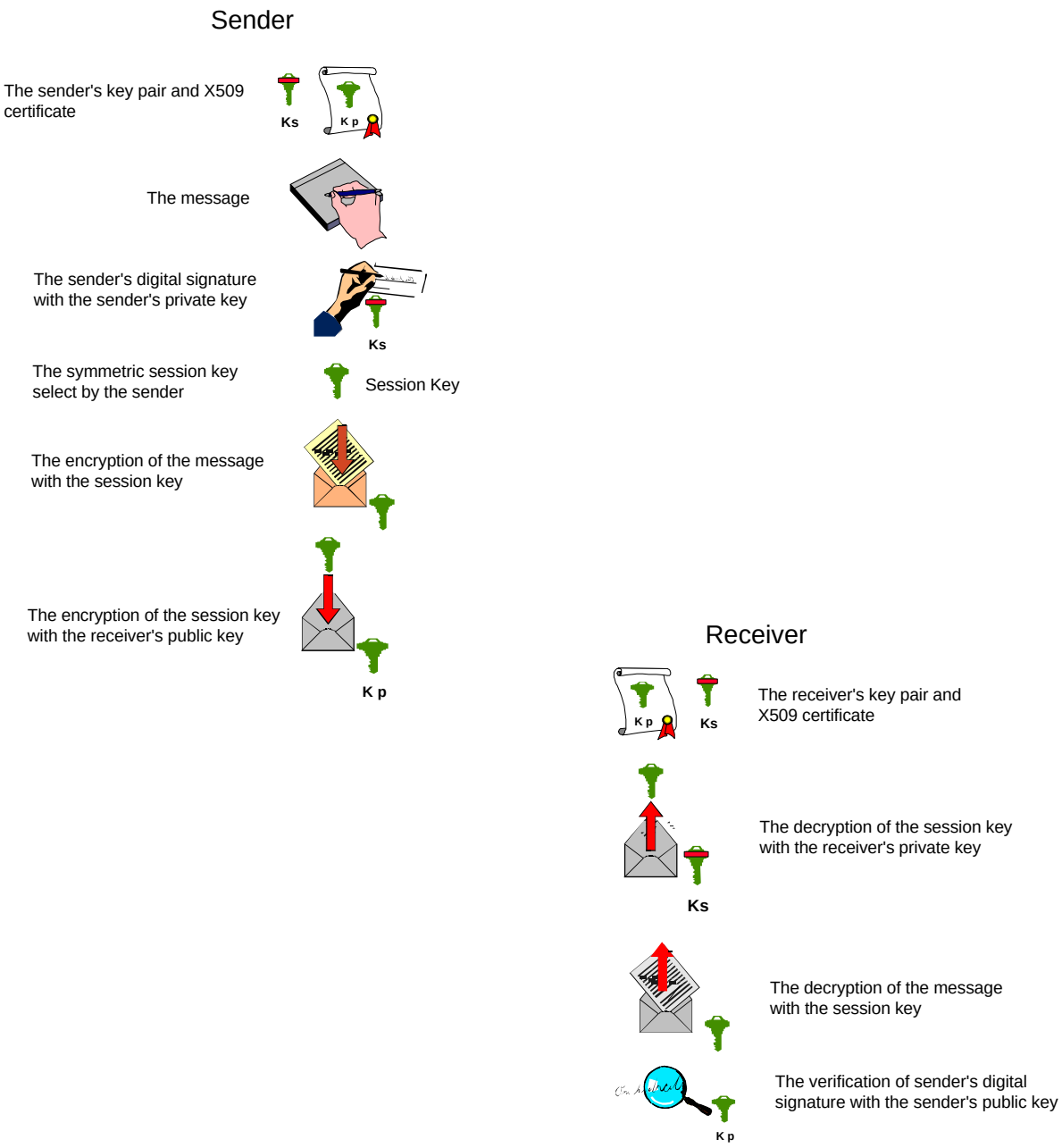
S/MIME uses a secure hashing function to detect message tampering.

3.13.4 Interoperability

Because S/MIME is an open standard, the mail software client can inter-operate with other S/MIME-compliant clients.

In addition, X.509 certificate support helps ensure that your users can send and receive signed and encrypted messages.

3.13.5 S/MIME flow decomposition



4. Setting up a GemSAFE application

4.1 GemSAFE: A service provider's view

Although GemSAFE is a turnkey client security solution, a certain amount of standard internet infrastructure is required in order to support it. The person who provides this infrastructure will be referred to as a *service provider* but may be a bank, an ISP, a company intranet administrator, an on-line magazine, etc. This person will provide a GemSAFE solution to a *community of end-users*.

The steps a service provider will follow are:

1. Select a CA infrastructure
2. Secure sensitive Web sites with SSL
3. Ensure users have correct E-mail infrastructure
4. Put other value-added services in place
5. Distribute package to end-users
6. Sit back and enjoy unrivalled E-mail and Web security!

These are described in more detail in the following sections.

4.2 Step1: Select a CA infrastructure

Since GemSAFE is based on public key cryptography, a certificate authority is required in order to manage certificates.

Let's look at the choices you have to make for issuing certificates. This can be represented by the matrix here below. Note that GemSAFE has been designed to fulfil the requirements of all these architectures.

	I'm my own CA		I replys on an external CA
	I buy a product	I outsource the service	
Users receive their cards preloaded with a certificate (off-line certification)	(1)	(2)	(3)
Users get their certificate on-line	(4)	(5)	(6)

Solution (1): You buy a CA solution to administer and operate the issuing of certificates in-house. You set your own CA policy. Gemplus will send you a batch of public keys and you generate the associated batch of certificates and send this back to Gemplus. Gemplus will then personalize the cards by downloading the certificate and possibly print the cardholder's name, expiry date, etc. Gemplus will then send the cards directly to people's home in a personalized mailing. Individuals get their personalized card and simply insert their cards to access their service. People may also receive their pin-code by a separate secure mailing.

Key points of this solution

+ you set your own CA policy,
+ you can re-sell CA services to other organizations,
+ your brand is perceived by the end-user as the reference as you are the trusted party,
+ service is simple and user-friendly for the end-user.
+ you are 100% sure the certificate is stored in the smart card,
= it is cost-effective for significant volumes only (above 10 ku),
- operating a CA requires significant resources.

Solution (2): You outsource the hosting of the CA solution. You usually pay on a per certificate basis. You can remotely administer and operate the issuing of certificates. Your CA operator generates certificates on your behalf and you set your own CA policy. Gemplus will send your CA operator a batch of public keys and your CA operator generate the associated batch of certificates and send this back to Gemplus. Gemplus will then personalize cards by downloading the certificate and possibly print the cardholder's name, expiry date, etc. Gemplus will then send the cards directly to people's home in a personalized mailing. Individuals get their personalized card and simply insert their cards to access their service. People may also receive their pin-code by a separate secure mailing.

Key points of this solution

+ you set your own CA policy,
+ your brand is perceived by the end-user as the reference as you are the trusted party (the fact that the service is operated by a third party is transparent to the user),
+ service is simple and user-friendly for the end-user,
+ you are 100% sure the certificate is stored in the smart card,
= it is cost-effective for significant volumes only (above 10 ku),

It is the solution we recommend for consumer applications.

Solution (3): You rely on trusted third party (TTP): it can be a national CA, an international reference such as Verisign or GTE-Cybertrust. Certificates are signed in the name of the TTP and you, as an organization, trust this TTP. You usually pay on a per certificate basis. Administration and CA policy is set by the TTP itself and you must agree with the given conditions. Gemplus will send the TTP a batch of public keys and your CA operator generate the associated batch of certificates and send this back to Gemplus. Gemplus will then personalize the cards by downloading the certificate and possibly print the cardholder's name, expiry date, etc. Gemplus will then send the cards directly to people's home in a personalized mailing. Individuals get their personalized card and simply insert their cards to access their service. People may also receive their pin-code by a separate secure mailing.

Key points of this solution

+ service is simple and user-friendly for the end-user,
+ you are 100% sure the certificate is stored in the smart card,
= it is cost-effective for significant volumes only (above 10 ku).
- you rely on the TTP CA policy

Solution (4): You buy a CA solution to administer and operate the issuing of certificates in-house. You set your own CA policy. Gemplus supply you with a batch of identical cards and you send these cards to your consumers. You then deliver certificates on-line, directly from your Web server. People have to go through the certification process themselves and the CA server should be able to control the input. This process may take time and is tedious for the end-user.

Key points of this solution

+ you set your own CA policy,
+ you can re-sell CA services to other organizations,
+ your brand is perceived by the end-user as the reference as you are the trusted party,
+ no personalization costs: no minimum card volume required,
- operating a CA requires significant resources.
- registration process may be perceived as tedious by consumers,

It is the solution we recommend for Intranet applications.

Solution (5): You outsource the hosting of the CA solution. You usually pay on a per certificate basis. You can remotely administer and operate the issuing of certificates. Your CA operator generates certificates on your behalf and you set your own CA policy. Gemplus supply you with a batch of identical cards and you send these cards to your consumers. Your CA operator then delivers certificates on-line, directly from its Web server: people have to go through the certification process themselves and the CA server should be able to control the input. This process may take time and is tedious for the end-user.

Key points of this solution

+ you set your own CA policy,
+ you can re-sell CA services to other organizations,
+ your brand is perceived by the end-user as the reference as you are the trusted party,
+ no personalization costs: no minimum card volume required,
- registration process may be perceived as tedious by consumers,

Solution (6): You rely on trusted third party (TTP): it can be a national CA, an international reference such as Verisign or GTE-Cybertrust. Certificates are signed in the name of the TTP and you, as an organization, trust this TTP. You usually pay on a per certificate basis. Administration and CA policy is set by the TTP itself and you must agree with these conditions as is. Gemplus supply you with a batch of identical cards and you send these cards to your consumers. TTP then deliver certificates on-line, directly from its Web server: people have to go through the certification process themselves and the TTP server should be able to control the input. This process may take time and is tedious for the end-user.

Key points of this solution

+ no personalization costs: no minimum card volume required,
- registration process may be perceived as tedious by consumers,
- you rely on the TTP CA policy

4.3 Step 2: Secure sensitive Web sites with SSL

In order to secure a Web site, no special software is normally required. Simply configure a standard Web server (Netscape, Microsoft, etc.) to enable SSL. Typically a Web site should be configured to accept SSL3 connections only (not SSL2, TLS, etc.), to accept only encrypted communication (key length subject to export laws) and to always demand client authentication.

The server needs to be configured to decide upon which CAs he accepts. This will typically be the only CA decided upon in the previous step. Once client authentication has been validated, many Web servers allow the mapping of a certificate to a user account on the server. This allows finer access control than simply allowing all those who have a valid certificate access to a particular resource.

Each server used will also require its own private key and corresponding certificate (for the authentication of the server to the client). The server's documentation will explain how to generate a key pair and a certificate request. The CA used to generate the server's certificate must be accepted by all the end-user's browsers. Because both the Microsoft and Netscape accept, by default, several CAs, it is usually advisable to use one of these. If another CA is use, the CA's certificate has to be securely distributed and installed in each user's browser.

4.4 Step 3: Ensure users have correct E-mail infrastructure

Since S/MIME is built on top of the standard MIME mail format, there is no additional work to do. The Netscape and Microsoft E-mail applications both dialogue with mail servers using the internet standard POP3 (Post Office Protocol). Any end-user with an account on a POP3 mail server can use GemSAFE!

S/MIME provides end-to-end security so any recipient of an S/MIME E-mail needs an S/MIME compatible mail application to fully decode the E-mail. However, if the E-mail is only signed (and not encrypted) then non-S/MIME mail users will be able to read the content but will not understand all the attachments. This can be useful when an existing community is making the transition to secure E-mail.

4.5 Step 4: Put other value-added services in place

The GemSAFE smart card can also be used for other things; for example it contains an electronic purse. This can be exploited as loyalty points for visiting a particular Web site, buying Web-based information, etc. This services require modification to the service provider's server software.

4.6 Step 5: Distribute package to end-users

The service provider will distribute to each end-user

- Smart card
- Card reader
- GemSAFE client software and documentation (+ browser if necessary)
- Server CA Certificate (if not a standard CA pre-installed in browser) *
- URL of the CA he is to use *
- One time password which enable the user to recover a certificate *

*= Optional

4.7 Step 6: Sit back and enjoy unrivalled E-mail and Web security!

Once the end-users are all up and running, the service provider will simply need to manage the addition of new end-users, lost cards, etc.

5. Gemplus and Internet applications

Gemplus has, since its inception in 1988, developed consumer products for financial institutions, Telecom Operators, Pay-TV operators, governments. These organizations require the highest product security and quality and regularly audit their key suppliers. The excellence achieved by Gemplus in these fields has enabled Gemplus to become the undisputed world leader of the smart card industry.

Gemplus has been the first company together with Hewlett Packard to strongly believe in the necessary integration of smart cards in IT systems. This strategic partnership has lead to the release of the very first Smart card enabled solutions for the Web in 1997: ImagineCard Web. For the first time, a service provider could buy a comprehensive system and not only components such as cards, readers, software, administration platforms to be integrated. To address the various needs of the IT market, Gemplus has also developed key partnerships with world-class leaders in their respective areas: IBM, Verifone, Verisign, Sun, Microsoft, Security Dynamics, Netscape and others.

Building on this expertise, Gemplus has designed GemSAFE to be the most secure, simple and plug-and-play solution. With GemSAFE, Gemplus offers a state-of-the-art solution to Internet service providers who need to deliver valuable Web services to consumers and employees alike.

GemSAFE, Web services in total confidence.