Identity Management

SECURITY KIT

SafeNet®
The Foundation of Information Security

SafeNet is a global leader in information security.

SafeNet provides complete security utilizing its encryption technologies to protect digital identities, communications and intellectual property, and offers a full spectrum of products including hardware, software, and chips.

SafeNet technology is the de facto standard in remote access client software and the market leader in USB authentication tokens that eliminate user names and passwords; SSL acceleration devices providing fast and secure online transactions; software security, and licensing products preventing software piracy; high-assurance security products; and SecureIP Technology licensed to Internet infrastructure manufacturers, service providers, and security vendors.

Table of Contents

Best Practices in Identity Management

There are many definitions, both academic and scientific, for 'information security'. Some are technical, some are even philosophical — most are difficult and obscure. So much so that the underlying purpose of security is often lost. It is actually very simple. The purpose of information and computer security is simply to ensure that the right people have the right access to the right information whenever they need it. ecurity is nothing more than ensuring this, and preventing everything else.

This basic principle applies whether it is your own staff accessing your own systems, or whether you are conducting electronic business with other companies. You need to know, with confidence, that people are exactly who they say they are; regardless of whether you are dealing with them, or they are dealing with you. You need to be able to manage 'identities'. Ensuring this is known as Identity Management.

Once a secure identity management system is in place, it can be developed into an enabler for other business practices beyond security. The foundation for it all, however, is the secure management of identities.

This paper will show first that the management of identities can and should be based on public key technology, and it will then discuss best practices for managing those identities within a public key infrastructure. In short, this paper discusses Best Practices in Identity Management.[1]

Public Key Cryptography and Infrastructure

We're going to start with an assumption: the assumption that the most efficient way in which to manage identities is within a public key infrastructure (PKI). This is actually a pretty safe assumption: the real question is not whether you need PKI to manage identities, but how you use PKI to manage identities.

But perhaps we do first need to dispel the persistent myth that PKI is too difficult, or too expensive, or unproven because of lack of adoption… all of these were once true. It used to be difficult because it was a technical solution to solve a business problem — and business is wary of technical solutions. It was once very expensive, because you had to go to a third party and pay for individual identity certifications. And because of this, business uptake of PKI was painfully slow in its early years.

But none of this remains true today — particularly since Microsoft has now built the heart of a PKI system into its Windows Server 2000 family. It is now a business solution; you do not need a third party; and no company running Microsoft Windows Server 2000 can have a valid reason not to implement a PKI as the basis of its identity management.

What is PKI and PKC?

A public key infrastructure is the infrastructure required to manage the use of public key cryptography. Public key cryptography was developed specifically to enable secure and trusted communication between individuals who may never have met each other. In other words, public key cryptography provides trust in identity.

It is based on the concept of a special and unique relationship between two distinct numbers. One of the numbers is made public (the public key), and the other is kept private. Only when the two are put together is the relationship seen to be true. It is also known as asymmetric encryption because it uses one key to encrypt and a related key to decrypt. (Symmetric encryption uses the same key for both processes.)

In practice, this concept usually uses two very large prime numbers. The product of these two numbers is an even larger number that has a unique relationship to its two factors. It is the unique relationship between the numbers that underlies public key cryptography. One related number becomes the public key, and one becomes the private key. Public keys are published, usually in LDAP directories, and are freely available. Private keys are kept strictly private and secret to the owner. But knowledge of both is required for both encryption and decryption.

If I wished to send you a confidential message, I would encrypt it using your public key as the encryption key, and send it to you. Only the owner of the corresponding private key would be able to decrypt that message. In other words, I could have trust in your identity even if we had never met.

In reality, I would not use PKC to encrypt my message. It has many advantages, but processing efficiency is not one. In reality, I would use an efficient symmetric algorithm to encrypt the message, and then use your public key to encrypt the symmetric key — and send them both to you. Only you would be able to get hold of the symmetric key to decrypt the message.

So far, I can use PKC to ensure that only the identity I intend (you) can read the message I send. But you cannot yet be certain that the message has come from me and no-one else (after all, it simply uses your public key, and anyone can get hold of that).

But PKC can also be used by me to digitally sign the message. To do this I first use a second mathematical function on the message, a hash function, to create a hash or message digest. The hash function should have two particular qualities: it should be 'collision free' (that is, no two messages should be able to produce identical digests); and it should be 'one-way' (that is, although you can obtain the digest from the message, you cannot obtain the message from the digest).

[1] For the purposes of this paper, when we talk about 'people', we also mean the computer processes that people control or instigate. Strictly speaking, when a person accesses a web page, it is the browser running on that person's computer that actually does the accessing. Nevertheless, if we have trust in the identity of the person controlling the processes, we can trust the process. If we do not have trust in the identity of the person, we cannot trust the processes. It still comes down to Identity Management.

This time, I encrypt the digest with my private key. You can then obtain my public key from the published directory and use it to decrypt the digest. You would then use your own private key to (obtain the symmetric key to) decrypt the full message itself, and then run the same hash function on the plaintext of the message. If the digest you obtain is the same as the decrypted digest sent with the message, then you will know that only I could have sent the message — since only I know the private key corresponding to my public key, and only I could have encrypted the original digest.

What I have done is to bind myself, through my PKC credentials, to the message. I have digitally signed it.

This may seem very complex — but in reality, the PKI software does all the work. It is effectively transparent to the user.

The Root Key

So, in summary, PKC enables me to be certain that when we communicate electronically, you are who I think you are; while you can be certain that I am who I say I am[2]. We have created trust in identity.

But there is one further hurdle to overcome: we need to be certain that the keys in question really do belong to the people who claim ownership of them. This is effectively done by a Certification Authority (CA) issuing a digital certificate to confirm that the keys in question really belong to that person. The digital certificate

- identifies the issuing Certification Authority
- identifies the certificate owner
- contains the certificate owner's public key
- is digitally signed with the Certification Authority's own private key.

If the CA is our own company, then we can trust all the keys issued to company personnel signed by the company CA. Other companies, however, may not so readily trust our own CA. We must therefore obtain verification of our CA from a third party CA that everyone trusts (there are numerous, such as VeriSign, GlobalSign, Thawte and others).

In such circumstances, where the company acts as the CA, the company's own public/private key pair is known as the 'root key' since it verifies all of the other keys.

Identity Management based on PKC — Best Practices

So far we can see that we can obtain trust in identity through the use of PKC. But this is not a paper on public key cryptography per se, it is a paper on Identity Management.

Our identity is based on the pairing of a public encryption key and a private encryption key. What follows as surely as night follows day is that Identity Management revolves around those keys: ensuring that the keys are generated securely, stored securely, distributed securely, and used securely. More than anything, that security must apply to the root key: if the root key cannot be trusted, then no certificate signed by that root, and no identity assured by the certificate, can be trusted.

It is against this background that we offer the following Best Practices in Identity Management.

1. Best Practice: Use PKI Technology

The first rule for best practice in identity management is to use public key cryptography and a public key infrastructure. The technology is proven, it is well established, and it provides all the facilities required for identity management.

2. Best Practice: the Certification Authority and Key Management

2.1 Use hardware for key generation and key storage

The entire security structure is built upon the foundations of the public and private keys. The public keys are not a problem since it is necessary to make them freely available. The private keys, however, must be kept strictly private, secret and secure — or you have no security.

The secure generation and storage of these keys is therefore paramount.

The options are to do this in software running on your system's operating system; or to do it within a separate hardware security module (HSM) that is securely connected to the system. There's clearly little difficulty in making the choice — in fact the only advantage of doing it in software is that it is cheaper. However, given all the security vulnerabilities that are regularly reported for all operating systems, this is not a very good choice. An option that some companies follow is beginning a deployment without an HSM and storing the keys on software and later importing them into an HSM. This is weak practice as there is no guarantee that the key that is protected by software hasn't already been copied.

"An HSM is a dedicated hardware device that is managed separately from the operating system. These modules work with any Windows Server 2003 CA to provide a secure hardware store for CA keys."[3] These modules also work with Windows 2000. However, it is still important that you choose the right HSM. The following are some of the features to look for.

2.1.1 Hardware-Secured Key Generation

Keys must be generated on a secure key management device.

This is the basis for trusted identity management. It is many, many times harder (if not ultimately impossible) to secure a general purpose server or any application running on that server, than it is to secure a purpose built separate security module. Ideally, the HSM should include its own random number or seed generator to provide a random key seed.

[2] It has other advantages — not least that it can confirm that the message has not been altered by any third party in transit (any alteration to the message would create a different message digest to the one enclosed with the message itself); and that it provides the basis of non-revocation (since you can prove that I sent it, I cannot later claim that I never said such a thing).

2.1.2 Hardware-Secured Key Storage
The Key must always be stored on a secure HSM.

As soon as a key is stored on a host server, it becomes vulnerable. It could get copied onto a vulnerable tape or disk backup system. It could be stolen through a remote access Trojan or simple social engineering. And once stolen, even if encrypted, the hacker has time to crack the encryption at leisure. It is important, therefore, to choose a hardware module that never copies the keys to the server.

If you use software key storage and backup this file, you run the risk if you need to use backup tape, of introducing keys that have been deleted. Unless a new backup tape is generated each time an update is made. Hardware key storage and backup removes this risk.

2.1.3 Hardware-Secured Key Backup
When Private Keys are backed up, they must be backed up to another identical security device.

Although the keys should not be backed up to the host server, nevertheless basic good security practice demands that there is a backup for disaster recovery purposes.

It follows that the backup must be just as secure as the primary storage. The ideal solution is thus to be able to backup your keys to an identical HSM — and to be able to do this via hardware and not via the host server.

Since general security good practices require that backups are not stored in the same location as the primary storage, and since we have already seen that the keys must always be stored in hardware, then it is clear that we need some way to transport the keys from primary to backup storage in hardware.

One solution would be to use a security token, whether that be a PCMCIA token or a smart card. We will see later in this paper that the use of compatible security tokens is necessary to achieve best practices in identity management. It follows that the use of similar tokens to transfer keys from primary to an identical backup storage would fulfill the requirement for a hardware-secured backup.

2.1.4 Hardware-Secured Digital Signing
All certificate signing operations must be performed exclusively within the HSM.

There are two reasons for this. The first is simply 'performance'. Certificate signing is processor intensive. And the longer the key, the greater the processing. According to Microsoft, "a short key length (512 BITS) generates very little CPU utilization." But it is recognised that keys should be at least 1024 BITS in order to provide adequate security. At this length there is a significant load on the CPU — and it is not something that can be solved by simply increasing the server's RAM. "The larger the signature key length, the greater the CPU utilization. Larger keys degrade CA performance. To be CPU-independent, you may want to use hardware acceleration to provide a large number of both key generation and signing operations."[3]

The simple fact is that you need to offload all cryptographic functions to a dedicated HSM with its own dedicated crypto processors in order to ensure adequate performance and to prevent overloading the host server.

The second reason that all certificate signing operations need to be performed within the HSM has already been discussed: basic security. In order to be signed on the host, the key has to leave the protection of the HSM and reside in the less secure host server. Best practice dictates that this should not happen.

2.1.5 PKI — Authenticated HSM Software Updates
All software code on the HSM should be authenticated through a trusted source and verified for integrity.

One of the primary reasons for using an HSM is that it is easier to secure than a host server. But that means that you have to trust the software that already exists on the HSM, and you need a secure method of updating, revising, and adding new functionality to that HSM.

If you cannot trust the software that is delivered, then you cannot trust anything that comes from that software. The first requirement is therefore to ensure that you have confidence in the HSM software, and how it is loaded into the HSM during manufacture.

The second requirement is that you must have confidence in the continued integrity of that software. One solution here could be the built-in use of a cyclic redundancy check (CRC[4]) to verify the code being used against the original in firmware.

The last requirement is that you also need a secure method for updating the software. If you are expected to download unsigned and unencrypted updates across the Internet onto your host server, and then to transfer the update to the HSM, then you do not have a secure hardware security module, and you do not have any identity-based security. This white paper describes best practices in PKI-based identity management. Since at this point we are attempting to ensure the 'identity' of software revisions and updates, it follows that HSM updates should be PKI-authenticated through a trusted source.

2.1.6 Physical Security
The HSM must be FIPS 140-2 validated or equivalent to provide additional security from direct physical attack; areas where the HSM is stored should be protected from unauthorised physical access through the use of facility access controls.

Any attacker with direct access to any hardware device has a far greater opportunity to compromise that system than one who

[3] Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure. By David B. Cross and Carsten B. Kinder, Microsoft Corporation.

[4] "A cyclic redundancy check (CRC) is a type of hash function used to produce a checksum, which is a small number of bits, from a large block of data, such as a packet of network traffic or a block of a computer file, in order to detect errors in transmission or storage. A CRC is computed and appended before transmission or storage, and verified afterwards to confirm that no changes occurred." Wikipedia.

has only indirect access. The physical security of the HSM is therefore to be taken seriously. This really has two areas: the HSM itself, and the location of the HSM.

For the first, you should seek a device that provides built-in tamper-resistance and tamper-evidence. Tamper-resistance can include features such as secure mounting, and the ability to lock the token reader to prevent unauthorised removal of tokens. "Tamper-evidence" features let you know if an unauthorised person has physically manipulated the device.

The location of the device should also be protected through some form of facilities control. The ideal solution is to keep the HSM in a locked room segregated from normal network appliances and routers that is only accessible via at minimum the presentation of an authorised user's token or at maximum some form of biometrics.

2.1.7 Host Independent Two-Factor Authentication
Login and authentication procedures must be performed independent of the host server, using two-factor authentication, through a trusted connection path to the HSM.

The primary function of almost all of these 'best practices' is to protect the integrity of keys held in, or generated by, the HSM. It follows, then, that it is essential to control user access to the device. Best practice in access control dictates two-factor authentication. But note that the authentication must be host-independent, using a trusted connection between the HSM and the authentication device.

Two-factor authentication involves the use of any two of the following authentication methods:

- something you alone know (such as a password or PIN number)
- something you own (such as a USB token or smart card)
- something you are (biometrics, such as a fingerprint or iris scan)

It doesn't really matter which two of these three factors are used; but it is worth bearing in mind that biometrics is still not widely deployed, is still subject to potential false positives and false negatives, and introduces a significant extra cost.

2.1.8 Enforced Operational Roles
To prevent unauthorized, unilateral actions by a single individual, operational roles must be split so that no one individual has too much operational control.

The usual assumption about security is that its purpose is to prevent outside intruders gaining access to sensitive inside information. This is clearly true. But almost all security surveys consistently demonstrate that the greatest security threat comes not from outside but from discontent or simply naive insiders — that is, your own employees. An effective means of minimising this 'insider' threat is to prevent too much operational control being focused in a single person. This is generally known as the 'separation of operational roles'.

It is therefore good practice to seek an HSM that provides for enforced operational roles in its use. Some of the roles normally present in the operation of a hardware security module include:

- key authentication
- initialising the token during setup
- token configuration and security management
- administrative and operational use
- backup and disaster recovery functionality

Best practice dictates that any one person should be authorised for as few as possible (preferably no more than one) of these roles. The result would be that serious unauthorised manipulation would require the collusion of more than one member of staff — which in turn is far less likely than the existence of a single malcontent.

2.1.9 FIPS 140-2 Validation and other validations
The HSM used for Private Key operations and storage must be FIPS 140-2 validated.

FIPS Publications are Federal Information Processing Standards. These standards are developed by the US National Institute of Standards and Technology (NIST) for US Federal computer systems. They have become, however, a general standard against which different systems can be rated.

The FIPS standard for cryptographic modules is FIPS 140-2. It contains 4 security level ratings, 1 to 4 from lowest to highest. Best practice would suggest that you use an HSM that conforms to FIPS 140-2 Level 2 as a minimum; and preferably (or at least in the important areas) FIPS 140-2 Level 3.

FIPS doesn't only control the physical security but also ensures correct operation of the algorithms and correct design of the software and device.

An alternative to the FIPS validation is Common Criteria (CC), and if an organisation is looking for an HSM with Common Criteria validation they should look for CC EAL4 or EAL4+.

There are many other validations however FIPS and CC are the two validations that are established and credible throughout the world.

Although certifications are a good baseline you should look what additional controls and functionality the vendor has placed above and beyond the requirements laid out in such certifications to ensure the security of keys and data.

2.1.10 Independent 3rd Party Audit
The presence of an external independent auditor during the Root Key generation ceremony, coupled with ongoing annual security audits, provides assurance and integrity for the Root Key and PKI.

Security, like justice, should not merely be done; it should be seen to be done. And you need to be able to confirm, independently, that it has been done. This requires the use of independent, external auditors firstly to be present at, and to witness, the major events (such as the root key generation); and then to

undertake and provide reports on regular security audits. This is not merely best practice, it is good governance and is increasingly required. You need it not merely for your own peace of mind, but to satisfy your customers and suppliers; and where applicable, your shareholders.

Look for an HSM that helps simplify the audit process. The HSM should provide a clear way to allow important operations such as key generation, backup and restore operations to be properly scripted and witnessed. Ideally this process should be done following a script, with each operation being witnessed and controlled. For audit purposes an HSM with a command line based management system is much better than a GUI one, even if GUI is more user friendly. This is because command line is easily auditable (it is easier to say 'at this prompt type x' than it is to 'click x tab, select x from the second pull down box on the right'). Plus a command line based system can be logged to a file and the file can be manually or digitally signed and archived.

2.2 Use a hardware token for user identification
Access by an individual to any facility, whether it be a building, a room or a computer, should require two-factor authentication (see 2.1.7 above for a brief discussion of this) in order to adequately confirm the identity of that individual. The two most commonly used factors in identity authentication are a password (something you know) and a hardware token (something — a smart card or a USB token — that you have).

Many of the best practices described in section 2.1 above apply equally to access tokens since these are also hardware devices storing digital credentials. It is the primary function that differs: the token is primarily to identify the holder.

However, the use of tokens to identify individuals presents its own challenges, and carries its own set of best practices. The challenges include:

- Provisioning
- Token and credential recovery and temporary replacement
- Token and credential cancellation/revocation
- Credential replacement or updates
- Token unlocking
- Applet management

2.2.1 Best practices in credential provisioning
A token is a versatile device, and can contain a considerable amount of information. This information could include PKI certificates and keys, symmetric keys, employment information and more. Getting that information onto the token is part of what is now known as 'provisioning'; that is, ensuring that everyone within the organisation receives (is provisioned) with what is necessary to undertake his or her responsibilities.

Many organizations that rely on simple passwords for access control and identity management have adopted centralised systems to automate the process of provisioning and managing passwords. Organisations that have turned to two-factor authentication for best practices in identity management are now considering solutions for automating the provisioning and managing of tokens. It is important that the system adopted can interface with different parts of the organisation in order to provision individual tokens easily, rapidly and inexpensively. This will require a consolidated provisioning system that can securely interface with the HSM, Human Resources, the master access control system, user directories and any other system in the organisation that leverages or interacts with the identity on the token.

There are two main steps to token provisioning: provision the physical token to the user, and provision the user's credentials to the token. Which of these steps occurs first depends on several things including corporate security policy and whether or not provisioning will be performed in a centralized manner, distributed manner or even a self-provisioning manner..

Centralized provisioning is when the tokens are all provisioned with user credentials in one location and then distributed to the end users. In this case the issuer must ensure that the authorised user actually receives their smart card and that it is not compromised en route. Creating the tokens with a one-time use PIN and distributing it in a PIN mailer is a common way to securely deliver tokens to remote users.

Distributed provisioning allows for multiple token issuance points, and relies on the user collecting the token personally. In such a situation, the loading of the user's credentials onto the token is often done over some portion of a public network and over a great distance; therefore, it is essential that a secure and trusted connection can be made between the source of the credentials and the location of the token.

Self provisioning allows for the user to be sent an empty token with some authentication information. They can then (typically) visit a web site which verifies their identity and locally provisions the token or card. This avoids local visits to provisioning centres.

Each method has advantages and disadvantages — but in reality, few companies would be able to rely on just one or the other. The provisioning system should therefore be able to provide both methods of token distribution.

2.2.2 Best Practices in token and credential recovery and temporary replacement
One issue with identity tokens is that they can be forgotten, or left at home; temporarily mislaid rather than permanently lost. Having to cancel tokens on all such occasions and generate new ones would be a costly and time-consuming affair.

It is good practice, therefore, to use a system that can easily and rapidly issue a temporary token or a password with limited capability in order to minimise the user's 'downtime'.

2.2.3 Best Practices in token and credential cancellation/revocation
On those less frequent occasions when a token is permanently lost, destroyed, stolen, or the token's owner is no longer with the company, then best practices require simple and immediate certificate revocation and to be able to update back-end applications automatically with this change.

Frequently, however, it is not the entire token but just part of the contained credentials that need to be cancelled. Best practice would therefore demand a system able to cancel the entire token. This is, in one sense, the reverse of provisioning.

Most critically, however, the system needs to be able to revoke any digital signatures contained on cancelled tokens with immediate effect. This will require not just the publication of revoked details on the PKI revocation list, but pushing out the details to all subordinate PKIs — immediately.

Best practice requires a flexible, efficient, but especially a rapid means of token or credential revocation.

2.2.4 Best Practices in credential replacement or updates
Just as there are legitimate reasons for revoking some of the token's credentials, so there are reasons for altering existing or adding new credentials. Certificates expire (traditionally, although not necessarily, certificates only run for a year before needing to be renewed); staff get promoted; or roles get redefined.

Once again, you need a system that can update just some of the credentials held on the token, and a system that can handle both centralised and distributed dissemination of updated credentials.

2.2.5 Best Practices in token locking and unlocking
Users will forget their PIN numbers. The first 'best practice' is that tokens should automatically lock after a definable number of incorrect PIN entries. This is to prevent a thief using brute force trial and error to obtain the number. But this security practice can lead to a large number of locked tokens.

If it is so relatively easy to 'lock' tokens, it must also be relatively easy — but secure — to unlock them. You therefore need a system that can easily, but securely, unlock tokens that have been locked without causing an excessive load on the support staff, and without causing extended 'downtime' for the forgetful user.

2.2.6 Best Practices in applet management
The versatility of the smart card and now USB token does not stop with its ability to store data — the inclusion of different Java applets allows it to operate as a miniature computer. This can increase the functionality of identity management to include features beyond security and identity proper. Java applets can allow the inclusion of cafeteria or staff refreshments programs, company benefits programs or even a corporate credit card.

This is an attractive facility — but if it is to be incorporated it should be part of the standard token issuance process. By their nature, of course, such things are apt to change and evolve, so there should also be the facility for easy updates to the token.

3. Conforming to Standards

A vital element in any computer system is its conformance to industry standards. We have already seen that it is important for the HSM used with a certification authority to conform to the FIPS 140-2 or CC EAL4 standard. But conformance of the Certificate Authority to all of the recognised PKI-related standards is essential. This is not merely to ensure the quality of the system itself, but to ensure maximum interoperability with other companies and their PKI systems.

It is also important to look for the vendor's attitude towards evolving standards — and an example in question could be the Federal Bridge. The Federal Bridge is a project in the United States to allow different PKI systems in different Federal agencies to interoperate. It is the CAs, not the individual users, that interface with the Federal Bridge. But because of the hierarchical trust model of PKIs, that effectively means that different organisations can trust each others' user certificates. This model is likely to become widely adopted within business.

Best Practice dictates conformance to existing and evolving standards.

4. Use the minimum number of different suppliers

One of the major problems with Identity Management is that there are many different companies providing bits of the solution. It is perfectly feasible to build an Identity Management system using different products from half a dozen different suppliers. There is a case in arguing for having many vendors in your infrastructure to avoid a compromise or weakness in one product. But there is one key problem here, in that the more vendors' products that are pieced together, the more the risk that there is a gap in security, and so the more likelihood of a breach in security. This risk is increased when updates are installed, since vendors do minimal inter- operability testing. Having a minimal number of suppliers reduces this risk and having a number of products from a single supplier will further reduce the risk of a security breach.

A further point to make is that the more companies that are involved, the greater the overall cost. This is not merely that the price you pay must support multiple company infrastructures, but that there is always a hidden cost in the effort needed to integrate and manage them all.

Best Practice dictates the use of as few different suppliers as possible.

Summary

This paper has discussed Best Practices in Identity Management. We can summarize these best practices as:

- use a PKI as the basis for identity management
- use a hardware security module to provide your own certification authority and key management
- use an integrated provisioning system for the users' card management
- conform to existing and evolving industry standards
- use as few different suppliers as possible.

If you adopt these best practices, you will obtain the most secure, least expensive, and most versatile identity management system for your own organisation — and one that is as far as is possible interoperable with other company identity management systems.

Identity Management Solutions from SafeNet

SafeNet secures digital identities

Most IT departments today have determined their need for an enterprise-wide identity management system. But too often the number one criterion when evaluating identity management systems is, "Will this solution allow me to more easily issue and manage digital identities to my fast growing end user population?" Many solutions exist today that meet this criterion.

In today's environment, where organizations are under increasing pressure to achieve legislative and regulatory compliance and maintain the security and integrity of valuable corporate data, the number one criteria should be "Will this identity management solution allow me to more easily issue and manage digital identities while ensuring the security and privacy of my users' identities and their information?"

Organizations don't just need Identity Management, they need Secure Identity Management. Knowing for certain that people are who they claim to be — even if you can't see them and even if you have never met — is the foundation upon which a secure business is built.

Until now, building a secure identity management system has represented a considerable challenge, with different pieces of the solution coming from different vendors, which brings with it a high risk of interoperability failure when each supplier releases new versions of their products.

Secure identity management consists of several different technologies that need to be made to work together. You need;

- cryptographic capability to generate, store and issue digital identities, ideally in the form of a separate hardware security module (HSM)
- identity tokens to hold the digital identity credentials and authenticate the identity of individual users
- a single sign-on capability to simplify the user's experience and ensure a consistent logon experience regardless of when and where they access the network
- a management system to control the entire lifecycle of the digital identities and the tokens
- full interoperability with Public Key Infrastructure technology to support the use of digital certificates as the trusted digital identity credential

SafeNet is the only company that provides all the components needed to secure and manage digital identities, thereby ensuring lower costs in terms of both deployment and ongoing maintenance. In addition, since all elements of the solution are provided by a single vendor, any risk of interoperability failure is minimised.

Luna SA and Luna PCI — Hardware Security Module (HSM)

The SafeNet Luna SA is a hardware security module (HSM) that connects securely via Ethernet to your network. The SafeNet Luna PCI is a PCI form-factor HSM device that is installed into your server. Both provide the following main features:

- hardware-protected security for your root and other sensitive corporate and server identity keys
- FIPS 140-2 level 2 and level 3 validation to satisfy the most stringent security policies
- contains its own cryptographic processor to reduce the load on the network server and provide the fastest possible cryptographic processing for
- key generation for user tokens
- digital signing operations
- SSL acceleration for web servers such as Microsoft IIS and Apache
- integrates fully with all the major CAs, including Microsoft Certificate Services, Entrust Authority, VeriSign, RSA, Nexus, Cybertrust, Open CA and many more.

iKey and Smart Card authentication tokens

It is computers that communicate with computers. Identity management therefore requires that you know who is using the computer that is doing the communicating. This is achieved with personal authentication tokens that contain the digital certificate of the user. The user needs to 'present' the token to the computer before being allowed to use it. SafeNet offers a choice of three tokens to cover all operational requirements: iKey 2032, the SafeNet Borderless Security 330 Smart Card, and the 330m biometric Smart Card.

iKey 2032

The SafeNet iKey 2032 is a USB-based portable PKI authentication token that generates and stores a private key and digital certificate on a device small enough to fit on a key chain. It provides the following features:

- eliminates weak passwords with two-factor authentication (access to the protected device requires both the token and knowledge of a unique PIN number)
- low cost solution since it does not require a separate 'reader'
- allows users to use different computers with complete security (the user doesn't have to be at his or her own computer to log onto the network)
- supported by hundreds of shrink-wrapped security applications, and also supports PKCS#11 and Microsoft CryptoAPI for easy integration into custom applications
- provides FIPS 140-1, Level 2 validated hardware security

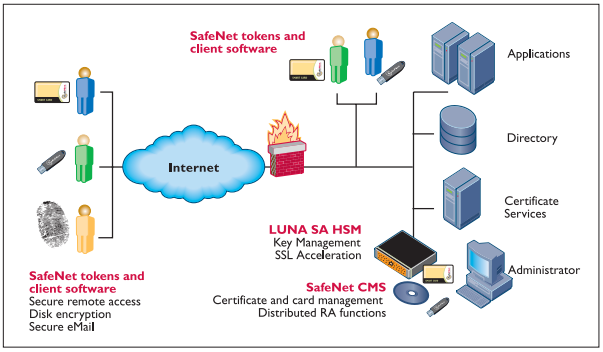


Diagram — Deployment Model with Luna SA

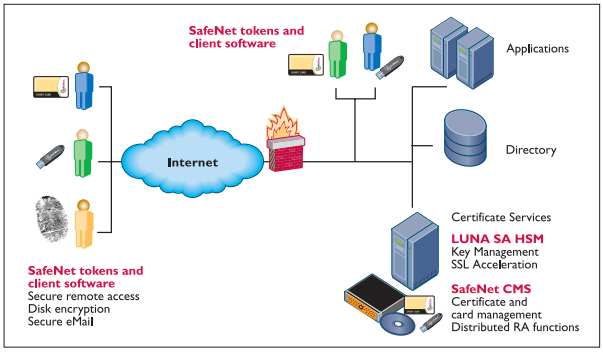


Diagram — Deployment Model with Luna PCI within a Microsoft environment

The iKey 2032 also can be Radio Frequency enabled so that it can be used as a physical access control device.

SafeNet Borderless Security 330 Smart Card

The SafeNet Borderless Security 330 Smart Card offers similar functionality to the iKey USB token, but does require a specific card reader. As a card it also provides the opportunity for user photographs to be included on the surface for badging requirements (so that the same card can double as an authentication device for computer access and an identification badge for facilities access).

SafeNet Borderless Security 330m biometric Smart Card

The SafeNet Borderless Security 330m Smart Card is a biometric-enabled Smart Card for use where maximum security is mission critical. Through the use of Precise Biometrics Match-on-Card™ fingerprint technology strong two-factor authentication is expanded into very strong three-factor authentication.

Axis single sign on

The SafeNet Axis system is a Smart Card/USB token based single sign-on facility. At one level it is a password management system ensuring administrative control over the company's passwords. But for the user it is a unified logon facility linked to the Smart Card or USB token. Once this link is established the process of user authentication through the token automatically allows access to the different systems that the user is authorised to use. There is no need to remember multiple User IDs and passwords, no need to interrupt work while signing on to a different part of the system. For the company it saves time and money; for the user it saves time and an awful lot of frustration. For both, it increases security.

Card Management System (CMS)

Digital signatures, private keys, certificates, authentication tokens… these are only part of the identity management concept. It's one thing to have these — it's a different matter to be able to manage and control them.

The SafeNet CMS is a web-based Smart Card/token and digital credential management system that draws everything together. It is used to issue, manage, and support SafeNet cryptographic Smart Cards and iKey USB tokens for identity-based applications throughout the organization. Its features include:

- provisioning — the CMS can interface with other parts of the enterprise, including, for example, the corporate HR system; thus ensuring that all employees can be speedily and accurately provisioned with their digital identity
- broad credential support — includes support for digital certificates, keys, passwords, biometrics, etc
- digital credential management — manages keys, certificates, and data on cards/tokens, including cancellation, temporary replacement, card unlocking and digital certificate revocation
- PIN management — reduces calls to your support desk caused by forgotten PINs
- flexible card issuance: tokens and cards can be generated from a central point for despatch to users, or from distributed points for collection by users
- card unlocking — reducing calls to the Help Desk when users forget their PIN number and lock the token with three incorrect guesses.

Deployment of SafeNet Identity Management Solutions
There are two basic deployment models depending upon whether a Luna SA HSM or a Luna PCI HSM are used. The diagrams above show the alternative options.

Summary

All of the above systems stand in their own right: hardware cryptographic processing for secure transactions and rapid SSL web functionality; two-factor strong access control with single sign on; and a digital credential management system. It is, however, only when you put all of this functionality together that you get true identity management. A common problem which occurs when an identity management system is constructed out of different elements from different suppliers, is that they never quite fit together seamlessly.

With SafeNet, the result is a complete, seamless, integrated and very secure identity management solution.

INA-Schaeffler

Deploys SafeNet's Luna SA Hardware Security Module to provide secure access to corporate data using digital certificates

INA-Schaeffler is a leading German supplier of roller bearings and high precision automotive parts. It employs over 28,000 people and operates 40 manufacturing facilities worldwide. Needing global access to corporate data around the clock for employees, sales agents, and affiliated companies, INA-Schaeffler required a method to secure access to their networks and facilities. With these goals in mind, INA-Schaeffler turned to ActivCard, Microsoft, and SafeNet to design and deploy a Public Key Infrastructure (PKI) to issue employees smartcards containing digital identities.

Although no bigger than a credit card, smartcards belie their diminutive size: consisting of tiny microchip embedded into a plastic card, each smartcard is a self-contained computer, complete with software, operating system, and storage capable of performing a specific set of operations in a secure environment. Most smart card operations revolve around performing cryptographic operations, for example, applying a digital signature to an electronic file. To do this, an electronic key stored on the smartcard is used to identify the signature holder and encrypt the document. The question of how those keys find their way into each smartcard can be answered by PKI.

PKI relies on asymmetric cryptography, a system that makes use of the unique relationship between a pair of cryptographic keys. These keys, a public key, and a corresponding private key, comprise a key pair. As their names suggest, a public key can be shared and distributed freely, whereas a private key must be carefully stored and kept secret. In a PKI, smarts cards are often used as an economical way to store private keys securely owing to their low cost and tamper-resistant hardware and software design.

As noted, public keys can be widely distributed. To do this, PKIs use certificates as a vehicle. Each certificate is a digital file containing a user's public key along with their name, address and other useful information. Like a driver's license, a certificate can be used during an online transaction as a form of identification. To prevent any from producing these digital identities, at the top of each PKI is a Certificate Authority (CA), a trusted, centralized certificate issuer, that functions like a license bureau.

To prove the authenticity of each certificate, the CA signs each certificate it issues with its own private key, and publishes its own certificate (containing it public key) so that its signature can be verified.

Because each PKI is a hierarchy, with all the trust inherent in the system resting on the trustworthiness of the issuing CA, the security of the CA's private key is paramount. Due to its significance, the CA's private key is referred to as the root key as it is the 'root of trust' for the entire PKI.

The Problem

INA-Schaeffler had an existing authentication system in place for remote access users but was disappointed with its operating costs and limited functionality. This system was built around portable tokens that display rolling one-time authentication passwords used to authenticate the user when logging into their network. This system required an additional authentication server and the tokens themselves had a limited lifespan necessitating costly replacement on a regular basis. The tokens also suffered from limited functionality; as they do not contain a digital identity tied to their owner, they could not be used to digitally sign documents or email. Their reliance on a manually entered PIN also made it difficult to use them to control access to buildings or other facilities. The decision was made to migrate to a smartcard based network authentication system that offered reduced costs while adding new digital signature capabilities and convenient physical access control features.

Deploying a smartcard system first requires a PKI to create digital identities (in the form of certificates) followed by a system to insert these certificates into smartcards before they are issued to employees.

After smartcards have been issued, the recipients require additional software that enables them to take advantage of the smartcards functionality on their computers. Deploying a PKI requires careful planning with attention to security and often requires the addition of numerous new pieces of software and hardware to existing IT systems. SM hardware. A proliferation of incompatible systems can add complexity and cost to smartcard deployments if the wrong components are selected and do not interoperate.

Fortunately for INA-Schaeffler, Microsoft, ActivCard, and SafeNet offer compatible components that simplify the deployment of a secure, comprehensive PKI and smartcard solution.

The Solution

INA-Schaeffler chose Microsoft Certificate Services for their Certificate Authority (CA). Microsoft Certificate Services is included as a service within the standard Microsoft Windows 2000 Server and Windows Server 2003 software package, allowing IT administrators to install and deploy a PKI to users without the need to purchase additional software. Microsoft Certificate Services tight integration with the Windows platform simplifies deployment and management to save time.

INA-Schaeffler's architechture relied on four CA's to handle specific tasks. A root CA was established at the top-level of their PKI hierarchy to issue certificates to three subordinate CAs. Each subordinate CA was responsible for handling certificate issuance duties for different groups of employees: one issues keys to executive and management staff, another to production employees, and a third to issue certificates to affiliate LUK.

To provide the most secure storage for the root key and subordinate CA signing keys, the SafeNet Luna SA network-attached HSM was the ideal choice. The Luna SA provides the strongest security for root keys while enhancing performance for demanding cryptographic operations, like digital signing, common to CA applications. Luna SA adds FIPS 140-1 Level 3 validated key management to the keys used by Windows Certificate Services. A fully integrated Microsoft CryptoAPI interface makes Luna SA plugand- play compatible with Microsoft's PKI services for rapid deployment.

INA-Schaeffler also made use of Luna SA's HSM partitioning feature. HSM partitions allow the Luna SA's single physical HSM to be subdivided into multiple logical HSMs. Each HSM partition maintains separate access and administrative policies to prevent sensitive key materials from exposure to unauthorized applications or administrators who need access to information on other partitions. INA-Schaeffler deployed two HSM partitions, one dedicated to the root CA, the second was shared between the three remaining subordinate CA's in their security architecture. The HSM partitioning, coupled with Luna SA's network interface, made it possible for one HSM to be shared between four applications, with INASchaeffler realizing a dramatic savings in equipment costs and maintenance as a result.

ActivCard's Identity Management System (AIMS) Enterprise Edition was selected to handle the issuance and management of INA-Schaeffler's new smartcards. AIMS was used to manage the issuance process and to insert certificates generated by the subordinate CA's into the smartcards during the issuance process. The smartcards themselves are dual-contact cards, featuring both a traditional contact interface for use with computers equipped with smartcard readers and a contact-less RFI interface commonly used with physical access systems.

Employees issued smartcards received Activcard Gold client software installed on their desktop PC's to provide smartcard login, password management, and application integration with the security and signing features offered by the smartcards.

Summary

With the help of ActivCard and SafeNet, INA-Schaeffler was able to deploy a PKI and smartcards to employees quickly and easily. These smartcards add security to their operations, enable digital signature integrity within electronic documents and email, and provide high-security access control to both computer networks and facilities. By using Microsoft Windows Certificate Services, INA-Schaeffler was able to leverage existing IT infrastructure and eliminate the need for additional CA software and licensing fees, saving time and money. The Luna SA provides FIPS 140-2 Level 3 validated security for the critical root key and subordinate CA keys to ensure that the digital certificates remain above compromise while HSM partitioning allowed for a centralized, easy to manage, cost effective HSM solution. ActivCard's AIMS Enterprise smartcard management system and ActivCard Gold client software provide a comprehensive solutions for back-office smartcard issuance and management and add smartcard security functionality to everyday user tasks like login and email.

Rabobank Group

Largest Dutch bank deploys 33,000 smart cards to authenticate internal users and secure online transactionsdata using digital certificates

"The SafeNet smart card meets our requirements for security, compliance with standards, role based access, and they're ready to go — what is called 'plug-and-play' in the industry.

In a highly distributed environment like ours, the smart cards are an efficient security solution."

Ad Bezemer,
Project Manager of Infra Services, Rabobank ICT

With 33,000 of its 50,000 employees worldwide serving 9 million customers in the Netherlands, Rabobank Group is the largest Dutch retail bank, operating about 1500 offices and 380 local banks.

From its roots as a Dutch agrarian cooperative providing credit to farmers over one hundred years ago, Rabobank today has grown to a position of world leadership as a wholesale bank to the global Food and Agriculture (F&A) and other emerging markets.

Rabobank Group's specialized banking businesses are market leaders in virtually all financial services — from leasing and trade finance to insurance, venture capital and private banking. Its century-proven customer focus and rock-solid practices have earned Rabobank Group the coveted AAA rating only bestowed upon a few banks worldwide by major credit rating agencies

Time-honored banking principles — trust and security — take on new significance in electronic age

Customer demands for trust and security have remained constant while revolutionary changes in banking practices and technologies over the past century have completely changed the culture of the industry. As more and more technology-savvy financial customers around the world expect to initiate secure transactions via the Internet or by phone anytime, anywhere, large financial organizations such as Rabobank Group, have put security strategies in place, both internally and externally, to keep pace with the technology requirements of electronic banking.

Rabobank Group has stayed several steps ahead of these increasingly complex technology challenges by consistently investing into a security infrastructure and strategy it calls Rabo Web Security (RWB), which is deployed enterprise-wide by its Zeist-based ICT Group. Working in close cooperation with Rabobank Marketing and listening to the specific local needs of its independent cooperative banks, Rabobank ICT is driven by the new market realities of electronic banking — declining numbers of bank offices and growing numbers of customers who opt for the independence and freedom of conducting increasingly complex transactions online.

"The bank's way of working today is quite different from the past and much more distributed," says Ad Bezemer, Project Manager of Infra Services at Rabobank ICT headquarters in Zeist. "Financial services have become much more complicated, as integrated products and several distribution channels are emerging. In the past, security meant shielding off hackers and intruders, but today, security means building the highest levels of trust right into our systems and communications."

Smart cards — security enablers in Rabobank's distributed environment

To build the highest levels of trust into its systems as it moves closer toward the future vision of 'anytime, anywhere banking,' Rabobank ICT has applied its forward-looking security strategy on several fronts, including its internal communications and channels. Since 1997, Rabobank-ICT has been moving all applications, which in the past had disparate security and required multiple passwords, to the intranet in order to make them available on all distribution channels. "This move enables us to centralize the security around these applications," explains Ad Bezemer.

To control access to these centralized applications and ensure strong authentication of its internal bank employees, Rabobank is deploying 33,000 smart cards combined with PKI (Public Key Infrastructure) technology that enable a new level of security and efficiency for its internal employees. The cards are provided by SafeNet, Inc., the leading North-American-based developer of smart card technology for securing e-business. SafeNet smart cards enable security in transaction- and communication-based domains such as finance, government, healthcare and telecommunications around the world.

At Rabobank, the deployment of SafeNet smart cards is eliminating the risks inherent in a "knowledge only" system based on multiple passwords, by providing two-factor security — something that is owned (the smart card) and something that is known (the user's password). In e-business security language, the smart cards provide 'non-repudiation' — two-factor security authenticates unequivocally that the user truly is who he/she claims to be — and therefore integrity and security. In addition, SafeNet smart card technology has FIPS 140-1 validation, an independent U.S. government certification of the

cryptographic strength and security provided by the SafeNet smart cards that is required by many financial organizations.

The SafeNet smart card technology deployed at Rabobank provides role-based access for users, which is particularly important at Rabobank because there are 55 different roles for its 33,000 employees in the Netherlands. The roles define what kind of transactions each user is able to conduct online. According to Rabobank's security policy, each application is classified with an internal classification system using the criteria availability, integrity and confidentiality (abbreviated in Dutch as the BIV code). On the highest security level, the BIV 3 classification, the smart cards are also used to add digital signatures to transactions. Its 32K-storage capacity easily allows the SafeNet smart card to store digital certificates with each internal user's role, as defined by the specific job level, as well as a high volume of updates.

"The SafeNet smart card is the enabler for Rabobank security," explains Ad Bezemer. "We are going from 10 to 12 different passwords, each application with its own authorization, to ONE smart card. The SafeNet smart card meets our requirements for security, compliance with standards, role based access, and they're ready to go — what is called 'plug-and-play' in the industry. In a highly distributed environment like ours, the smart cards are an efficient security solution."

Because Rabobank's cooperative banks decide independently on their local needs and requirements, some are using the smart cards for physical access. To meet the specific requirements of those banks, the smart cards are delivered custom-formatted with magnetic stripes and proximity technology. The SafeNet technology supports different kinds of readers and the smart cards are instantly deployable with the Compaq keyboard readers already installed at Rabobank, both at distributed sites and centrally. Whatever 'flavor' of smart card the individual banks prefer, employee uses include network access, Windows logon, and digital signatures. Rabobank has given several hundred additional smart cards to large customers for special transactions.

In international scenarios, for example, the smart card is used for 'dealing room' currency transactions. The customer is able to do an immediate buy or sell in the exact dollar (or other currency) amount without incurring the risk inherent in delayed transactions of losing funds through currency fluctuations. "By ordering the currency transaction directly with the smart card, the customer is able to side-step the process of calling the bank and arranging a transaction which may take a month or two to complete," says Ad Bezemer. "The usually 10-second confirmation makes the transaction almost real-time, versus the risky delays with the old process. The smart card offers our currency-trading international customers speed, cost-efficiency and transactional security."

Rabobank expects ROI from technology investments in trust and security

Rabobank is planning to move its web security strategy forward with several technology enhancements in the near term. Once every user has a smart card, this card will be the only authentication device for employees and can be used in other areas such as Remote Access, VPN and secure mail. The approximately 10% of Rabobank users who work in small offices or are mobile use the Citrix concept of Server Based Computing. These users will also be using smart cards for Remote Access and digital signatures.

As Ad Bezemer puts it: "Our role here at Rabobank ICT is to be enablers of methods and technologies that are vital to our business. The advance of e-commerce means a continued focus on the security of all transactions. Deploying the smart cards internally has been one important aspect of our security strategy. Now that we have laid the foundation, we can cash in on that and deploy on a larger scale. That's the nature of our business as a bank — to pay off, our communication has to be rock-solid, built on trust and security."

SafeNet Smart Cards

Locking the virtual door to unsecured online information and communications

Features

- RSA sign/decrypt — key lengths from 512 bits to 2048 bits
- DSA sign/decrypt — key lengths from 512 — 1024 bits
- DES/3DES encrypt
- On-card key generation
- SHA-1 cryptographic functions
- Multiple keys and certs (up to EEPROM limits)
- Validated to FIPS 140-2 Level 2
- PKCS#11 and MS-CAPI interface requirements
- GSA interoperability specfications
- User PIN unblocking
- Convenient ISO-compliant (7816) smart card format.
- Cryptographic co-processor for improved performance and speed.
- On-board DES hardware co-processor for secret-key encryption.
- 32K smart card operating system in ROM.
- 32K EEPROM for secure storage of keys, passwords, certificates, application programs and data.
- Implements public key functions:
  RSA/DSA key generation.
  RSA for digital signature.
  DSA for digital signature.
  RSA key exchange.

Diffie-Hellman key exchange.

- Hardware and software protection against differential power attacks and timing attacks.
- Validated for FIPS 140-2 Level 2.
- GSC-IS V2.1 Compliance
- Digitally signed executable programs provide card versions to support
  Identrus specifications.
  GSA multi-pin architecture.
  Biometric algorithms.
  Card unblocking

The power behind SafeNet's cutting-edge PKI smart cards is found in its smart card operating system, DKCCOS (Datakey Cryptographic Card Operating System), and embedded microcontroller—which contains a modular arithmetic processor and 32K EEPROM storage. The embedded microcontroller makes cryptography convenient to use and surprisingly fast. While the sophisticated token operating system resides in ROM, its capacity can be extended using nonvolatile EEPROM memory to securely store passwords, private keys, public certificates and other data as required. Digitally signed executable programs extend the feature set of the operating system providing card versions that support application specific requirements such as those for Identrus, Match-on-Card biometrics, card unblocking, and GSA. Plus, it has the flexibility to provide for future crypto-graphic functions and data management.

Security Services of SafeNet Smart Cards

User Authentication
SafeNet smart cards require users to authenticate themselves before initiating any security functions. Authentication is accomplished through the use of a password in accordance with the ISO 7816-4 smart card standard. SafeNet smart cards ensure that only authorized users can perform the cryptographic functions.

SafeNet smart cards provide confidence in online communications. They feature on-chip public key functions that support emerging public key challenge-response protocols such as FIPS PUB 196.

RSA/DSA Key Generation
The integrity of public/private key pairs is fundamental to the success of any crypto system. Keys that are stored on a computer and protected only by software are vulnerable to a number of hacking techniques and illicit "key-stealing" programs that can run undetected. Since SafeNet smart cards perform all sensitive cryptographic functions directly on the card — including public/private key generation, digital signature creation, and cryptographic session key unwrapping — unauthorized users have no way of accessing a user's digital credentials without stealing the smart card and guessing the pass phrase.

RSA/DSS Digital Signature
On-chip cryptographic functions allow users to produce either RSA (PKCS #1) or DSS (FIPS 186) digital signatures with confidence in the long-term secrecy of their private keys. Only smart cards can provide this long-term confidence in digital signature key sets.

RSA and Diffie-Hellman Key Exchange
No system is complete without support for the exchange of session encryption keys. SafeNet smart cards include both RSA key unwrapping and Diffie-Hellman key agreement and key exchange functions. The private keys used for these exchange functions are never exposed to a vulnerable host system.

Secure Storage

All of the cryptographic functions, operational parameters and general-purpose storage remain secure behind a "silicon firewall." This allows full customization of the smart cards to meet the requirements of specific applications. Implementation of customized security features and general-purpose data storage is in accordance with the ISO 7816-4 standard.

Configurability

SafeNet smart cards provide a token configuration file that enterprise security officers can use to permanently enable or disable cryptographic functions and to configure the tokens to match the security policy of the enterprise.

Software Support

SafeNet smart cards are easily integrated using included robust client middleware and drivers or with the SafeNet Borderless Security Single Sign-On strong authenti-cation and single sign-on software product.

Applications such as Netscape Communi-cator, Entrust Client and Microsoft Internet Explorer automatically make use of SafeNet smart cards when they are used with supporting client middleware software.

Technical Specifications

Standards

- ISO 7816-2 for dimensions and location of the contact (for smart card).
- ISO 7816-3 for electronic signals and transmission protocol type T=1.
- ISO 7816-4 for inter-industry commands of interchange security standards.
- FIPS PUB 186: Digital Signature Standard.
- FIPS PUB 196: Authentication using Public Key Cryptography.
- PKCS #1: RSA Encryption Standard.
- PKCS #3: Diffie-Hellman.
- PKCS #11: Cryptographic Token API Standard (CRYPTOKI).
- Microsoft Crypto API.

Electrical

- Power: 10 mA maximum.
- Supply voltage range: 5Vdc +/- 10%.
- Sleep mode: 200 uA max.
- ESD protection: > 4 kv.

EEPROM Memory

- Capacity: 32K
- Read cycles: Unlimited
- Write/erase cycles: 100,000

Environmental

- Storage Temp: -40°C to 125°C
- Operating Temp: -25°C to 70°C

Workstation Interface Smart Card Readers

- Serial reader
- USB reader
- PCMCIA reader
- Any reader that includes Microsoft PC/SC standards compliant reader drives

Benefits

Integrated Physical Security

Luna PCI is validated under FIPS 140-2 at both Level 2 and Level 3. All models are securely packaged inside specially designed enclosures to meet stringent requirements for tamper and intrusion resistance.

Plug and Play Support for Windows Platforms

Plug and play support for Microsoft Windows 2000, Windows XP, and Windows Server 2003 ensures easy deployment of Luna PCI to a wide range of security applications including IIS Server, Microsoft Certificate Services, ISA Server and RMS Server.

Full Cryptographic API Support for Easy Integration

Luna PCI supports PKCS#11, Microsoft CryptoAPI, Java JCA (Java Cryptographic Architecture), and Open SSL Cryptographic APIs to simplify development and speed application deployment.

Developer's Toolkit

For developers, the powerful easy to use Luna Toolkit is available to make it easy to add secure, hardware-based cryptographic processing to your custom applications.

Luna PCI

Hardware Security Module

Luna® PCI is a family of high-security cryptographic PCI accelerator cards—the same cards that power the acclaimed Luna SA Network HSM which is widely used by major governments, financial institutions and large enterprises around the world.

Hardware Key Management

Luna PCI offers dedicated hardware key management to protect sensitive cryptographic keys from attack. The high-security hardware design ensures the integrity and protection of encryption keys throughout their life cycle. All digital signing and verification operations are performed within the HSM to increase performance and maintain security. Luna PCI HSMs provide hardware secured key generation, storage, secure key backup and accelerated encryption in a range of models and configurations offering a wide selection of security, performance and operational capabilities.

High-Performance Cryptographic Processing

Luna PCI offloads computationally intensive cryptographic operations with dedicated hardware acceleration. Low-end Luna PCI models provide over 1200 asymmetric 1024-bit RSA operations per second to eliminate application processing bottlenecks for high-volume digital signing, encryption, and key generation. High-end Luna PCI models offer a blazing 7000 asymmetric 1024-bit RSA operations per second all under the security of FIPS validated hardware.

Certified Hardware

Luna PCI cards offer a wide range of premium security certifications including FIPS (Federal Information Processing Standards) 140-2 Level 2 and Level 3. Common Criteria at EAL 4+ and German Digital Signature Law are in progress.

Luna PCI is available in various configurations and certification levels to enable a wide range of security policies and operational practices.

Secure Authentication and Access Control

Luna PCI offers strong two-factor authentication and multiple administrator roles to prevent unauthorized access to sensitive cryptographic material. Luna PCI models supporting FIPS 140-2 Level 3 operation offer true Trusted Path Authentication using the Luna PED (PIN Entry Device) which is an integrated handheld authentication console that does not rely on commercial keyboards or displays for administrator PIN code entry.

Cryptographic Capabilities

Luna PCI supports a broad range of asymmetric key encryption and key exchange capabilities as well as support for all standard symmetric encryption algorithms. Luna PCI also supports all standard hashing algorithms and message authentication codes (MAC) as well as Random Number Generation based on Appendix A 2.4 of ANSI X9.31.

Secure Authentication and Access Control

Luna PCI offers strong two-factor authentication and multiple administrator roles to prevent unauthorized access to sensitive cryptographic material. Luna PCI models supporting FIPS 140-2 Level 3 operation offer true Trusted Path Authentication using the Luna PED (PIN Entry Device) which is an integrated handheld authentication console that does not rely on commercial keyboards or displays for administrator PIN code entry.

Cryptographic Capabilities

Luna PCI supports a broad range of asymmetric key encryption and key exchange capabilities as well as support for all standard symmetric encryption algorithms. Luna PCI also supports all standard hashing algorithms and message authentication codes (MAC) as well as Random Number Generation based on Appendix A 2.4 of ANSI X9.31.

Technical Specifications

Client API Support

PKCS#11 v2.01, Microsoft CryptoAPI 2.0, Java JCA/JCE, Open SSL

Operating System Support

- Microsoft Windows 2000,Windows XP,Windows Server 2003
- Linux Kernels 2.4, 2.6

Cryptographic Processing

Asymmetric Key Encryption and Key Exchange
RSA (512-4096 bit) (PKCS #1 v1.5, OAEP PKCS#1 v2.0) , Diffie-Hellman (512-1024 bit), DSA (512-1024)

Symmetric Algorithms
DES, 3DES, (double & triple key lengths) RC2, RC4, RC5,AES

Hashing Algorithms
SHA-1, SHA-256, SHA-384, SHA-512, MD-2, MD-5

Message Authentication Codes (MAC)
HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SSL3-MD5 MAC, SSL3-SHA-1-MAC

Random Number Generation

Luna PCI supports random number generation based on Appendix A 2.4 of ANSI X9.31

Physical Characteristics

Card type: PCI Card, 3.3V

Operating Temp: 0°C to 50°C

Storage Temp: -20°C to +65°C

Regulatory Standards Certification

1950 & CSA C22.2 safety compliant
FCC Part 15 — Class B

Benefits

Security

- The Luna SA's operational, software, and hardware design ensure the integrity and security of cryptographic processes and key material with multiple levels of security.
- Operational controls, including optional two-factor authentication and per-process software access, prevent unauthorized access and administration.
- The Luna SA's intrusion-resistant, tamper-evident seals chassis includes anti-tamper screws, probe-resistant baffles, and intrusion detection switches to provide both passive and active defence against attack.
- Secure software practices maintain system integrity with PKI-signed code modules to prevent the introduction of rogue software into the Luna SA.

FIPS 140-2 Validated

The Luna SA features an integrated FIPS 140-2 validated HSM to protect critical cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications. FIPS 140-2, Level 3 and FIPS 140-2, Level 2 variants are available to match the security profile of your specific applications.

Scalable

With a wide range of configuration options, the Luna SA scales to meet your demands as applications grow.

Luna SA

Network-Attached Hardware Security Module

A flexible, network-attached hardware security module featuring powerful cryptographic processing and hardware key management for applications where security and performance are a priority.

Secure Hardware Key Management and Cryptographic Processing

Luna® SA features an integrated hardware security module (HSM) offering hardware key management and cryptographic acceleration for unrivalled security and performance. Luna SA's built in HSM is FIPS 140-2 validated, capable of over 1200 operations per second (RSA 1024-bit), and offers optional standalone authentication (FIPS 140-2, Level 3 models only) to protect the most demanding security applications.

Network Shareable

The Luna SA includes Ethernet connectivity for flexible deployment using standard datacom cabling. Built-in support for TCP/IP (Internet Protocol) ensures that Luna SA deploys easily into existing network infrastructure and communicates with other network devices. Multiple application servers can share the Luna SA's cryptographic capabilities though Network Trust Links that combine 2-way digital certificate authentication and 128-bit SSL encryption to secure communication channels between the Luna SA and application servers, ensuring that sensitive data remains protected in transit.

Configuration Flexibility

Luna SA's flexible feature set is available to solve a wide variety of security problems. Luna SA's HSM Partitioning allows a single HSM to be divided into multiple logical HSM partitions. The Luna SA is available with up to 20 unique HSM Partitions, each with their own access controls and independent key storage.

Luna SA supports load-sharing and High Availability by allowing multiple units to operate in parallel to dramatically reduce the risk of a service outage as well as increased performance and throughput.

Multi-Level Access Control and Authentication

Multi-level authentication policies control access to the Luna SA's administrative functions to provide the highest degree of protection for sensitive cryptographic keys and prevent unauthorized system configuration changes while still permitting flexible remote management and monitoring. Access to sensitive HSM administration functions is controlled through the Luna PED (PIN Entry Device), a handheld, two-factor authentication device connected directly to the Luna SA.

iKey 2032
Certificate #161

Integrated Physical Security

Tamper-evident seals, intrusion detection switches, and shielded connectors designed into the Luna SA minimize exposure to direct physical attacks.

Simplified Remote Administration

The Luna SA features a Secure Command Line Interface (SCLI) to simplify remote system administration and streamline maintenance. A local console port is offered for secure initial configuration or direct system administration.

Backup and Disaster Recovery

The Luna SA's data contents can be securely stored on Backup Tokens to simplify backup, cloning, and disaster recovery.

Standard Cryptographic API Support for Easy Integration

The Luna SA simplifies integration and ensures application compatibility with support for PKCS#11, Microsoft CryptoAPI 2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions) and OpenSSL cryptographic APIs.

Luna Token Interoperability

To protect existing HSM investments, SafeNet Luna CA3 cryptographic tokens interoperate with the Luna SA through an integrated PC-Card token interface.

Industry Standard Rackmount Chassis

The Luna SA's 2U 19" rackmount chassis is optimized for accessibility, security, and dependability to meet the high processing density and manageability needs of corporate data centers.

Software Upgradeable

The Luna SA uses extensible Ultimate Trust Security Platform to add new functionality or increase performance. With PKI-signed software upgrades, new software features can be securely added, or existing configuration features can be easily deployed to units in the field.

Technical Specifications

Cryptographic APIs

PKCS#11 v2.01, Microsoft CAPI v2.0, Java JCA/JCE CSP, OpenSSL

Cryptographic Hardware Validation

- FIPS 140-2 Level 3 validated — certificate number 375
- FIPS 140-2 Level 2 validated — certificate number 436

Cryptographic Functions

- True hardware accelerated random number generation (Annex C of ANSI X9.17)
- Symmetric and asymmetric key pair generation
- Encryption and decryption
- RSA
- Digital signing

Cryptographic Performance

Over 1200 1024-bit RSA cryptographic operations per second

Cryptographic Algorithms

Asymmetric Key with Diffie Hellman (1024-4096 bit), RSA (512-4096 bit) and (PKCS#1 v1.5, OAEP PKCS#1v2.0), Digital Signing via RSA (1024-4096-bit), DSA (512-1024-bit), (PKCS#1 v1.5) and Symmetric Keys through 3DES, (double & triple key lengths), AES, RC2, RC4, RC5, CAST-128. Hash Digest is SHA-1, SHA-2 (160, 256, 512), MD-5 and Message Authentication Codes (MAC) are HMAC-MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Physical Characteristics

Connectivity
- 2x 10/100 Ethernet, CAT5, UTP
- Luna PED authentication port
- Local serial console port
- Luna Token PC-Card slot

Dimensions
- 2U full-length 19" rackmount chassis (ANSI/EIA-310-D compliant)
- 19.0" x 20.6" x 3.45" (482.6mm x 523.2mm x 87.7mm)
- 35lb (15.9kg)

Removable Storage
- PC Card Type II Slot, 5V (+/- 0.25V)

Temperature
- Operating 0°C to 40°C, Storage -20°C to +65°C

Regulatory Standards Certification

- U/L 1950 & CSA C22.2 compliant
- FCC Part 15 — Class B ISO — 9002 Certification

Benefits

Compact and Convenient

Although the SafeNet Borderless Security iKey 2032 USB Token is smaller than a stick of gum, it offers big security features. Its small size and rugged, tamper-resistant construction make it easy to carry so users can always have their unique digital identities with them.

Easy to Deploy USB Connectivity

The SafeNet Borderless Security iKey 2032 USB Token offers the security of a smart card without the need for a smart card reader. It features a built-in USB 1.1/2.0 port to easily connect to virtually any computer. There is no need to deploy and maintain costly smart card readers or special biometric devices to enhance your security applications— iKey offers smart card security without the headache.

Onboard Cryptographic Processing

Unlike other smart card or token-based authentication systems, the SafeNet Borderless Security iKey 2032 USB Token offers onboard key generation and cryptographic processing to ensure that cryptographic keys and functions remain secure at all times.

iKey 2032

Personal USB Authentication and Encryption Token

iKey™2032 is a compact, two-factor authentication token that provides client security for network authentication, e-mail encryption, and digital signing applications.

The SafeNet Borderless Security iKey 2032 USB Token is a USB-based portable PKI authentication token that generates and stores a private key and digital certificate on a device small enough to fit on a key chain. An extension of smart card technology, the SafeNet Borderless Security iKey 2032 USB Token simply plugs into any USB port and provides strong user authentication without the need for costly reader devices. The iKey 2032 USB Token is designed to support a wide range of desktop applications and portable systems. Its low-cost, compact design, and standard USB interface make it easier to deploy than cumbersome smart cards or one-time PIN tokens. Its FIPS Level 2 validated hardware and onboard key generation, key storage, encryption, and digital signing add high-assurance security to client applications.

Eliminates Weak Passwords with Two-Factor Authentication

SafeNet Borderless Security iKey 2032 USB Token brings two-factor authentication to applications where security is critical. Unlike traditional password authen-tication that relies on weak, easily guessed passwords, iKey 2032 USB Token requires both a physical token (the iKey itself containing the user's unique PKI key) and the user's PIN to complete the authentication process.

Supported by Hundreds of Security Applications

SafeNet has worked with software and hardware vendors to ensure that iKey offers the widest range of support for security solutions. iKey support is included in Single Sign-On/smart card login, VPN authentication, e-mail encryption, digital signatures, and many other PKI-enabled applications from leading vendors, such as Microsoft, Entrust, Computer Associates, VeriSign, and more. SafeNet Borderless Security iKey 2032 USB Token supports PKCS #11 and Microsoft CryptoAPI for easy integration into custom applications.

FIPS 140-1, Level 2 Validated Hardware Security

SafeNet Borderless Security iKey 2032 USB Token is FIPS 140-1, Level 2 validated to offer high-assurance protection for applications that require high levels of physical and operational security.

Compact and Convenient

Although SafeNet Borderless Security iKey 2032 USB Token is smaller than a stick of gum, it offers big security features. Its small size and rugged, tamper-resistant construction make it easy to carry so users can always have their unique digital identities with them.

Purchase a Complete Solution with Other SafeNet Products

SafeNet Borderless Security Single Sign-On, bundled with the iKey, provides strong authentication and Single Sign-On of user-names, passwords, and digital credentials stored using the iKey USB Token. Easy to install and maintain, Single Sign-On fortifies security with two-factor authentication and automated enforcement of strong password policies. The user simply inserts the token, enters a PIN, and the Single Sign-On software assumes all login and password management functions.

SafeNet Borderless Security iGate SSL VPN is the leading SSL VPN appliance, providing secure remote access to sensitive data. The SafeNet Borderless Security iKey 2032 USB Token enhances this security with two-factor authentication of the user's credentials. The iKey can store either the iGate password or a digital certificate—the user need only remember the PIN to unlock the iKey for simple and secure Single Sign-On to networksand applications.

Technical Specifications

System Requirements
Operating Systems Supported:

- Microsoft Windows 95, Windows 98, Windows NT (SP4), Windows 2000, Windows 2003, and Windows XP

Cryptographic APIs

- PKCS #11 v2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC

Cryptographic Hardware Validation

- FIPS 140-1 Level 2 validated — Certificate No. 161

Cryptographic Functions

- Asymmetric key pair generation (RSA)
- Symmetric key generation (DES, 3DES)
- Hardware-secured key management and storage
- Onboard digital signing

Cryptographic Performance

- 1024-bit and 2048-bit RSA key operations
- Key generation: Less than 90 seconds with key verification
- Digital signing: Less than 1 second

Cryptographic Algorithms

Asymmetric Key Encryption
- RSA 1024-bit, RSA 2048-bit

Symmetric Key Algorithms
- DES, 3DES

Digital Signing
- RSA 1024-bit, RSA 2048-bit

Hash Digest Algorithms
- SHA-1

Additional algorithm support available

Physical Characteristics

Hardware System
- 8-bit processor
- 32K memory

Connectivity
- USB 1.1/2.0 compliant
- 1.5Mbits per second transfer

Dimensions
15.875mm x 57.15mm x 7.9375mm

Regulatory Standards

FCC Part 15 — Class B CE

Custom brand graphics available

Benefits

Administrator Benefits

SafeNet Axis Rapid Deploy Technology™ automates policy, credential and desktop management through a single Management Center. Axis makes it easier to configure and deploy smart cards for access to a complete range of corporate resources.

Other benefits include:

- Applications and infrastructure remain unaltered
- Integrated PKI-based strong authentication and secure e-mail
- Policy-enforcing client softwareis transparently pushed to each workstation.
- Automated software and credential updates
- Automatic support of strong password policies and access policies are automatic
- Optional Microsoft and Citrix and terminal server support
- Corporate security is enhanced through secure Single Sign-On to Windows®, corporate applications, VPN/RAS remote access, Microsoft® applications and facility access control systems

User Benefits

Because a single PIN unlocks the credentials consolidated on the smart card or token and automates sign-on to corporate resources, it eliminates the need for employees to remember multiple passwords. Thanks to drastically reduced password issues, businesses become more productive.

Company Benefits

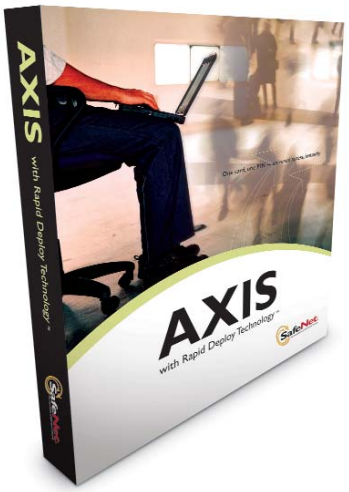
Large and medium-sized enterprises benefit from rapid Return-on Investment thanks to:

- Significant reduction in administrative workload, enabling IT to focus on business-critical activities.
- Enhanced user productivity and simplification of access.
- Stronger security and oversight of all access and identities.

Axis

Strong Authentication and Single Sign-on

SafeNet Axis™ offers critical advantages. The smoothest integration. The fastest deployment. The easiest management. The simplest operation. The highest Return-on-Investment. And the strongest access security. All from a single point.



SafeNet Axis Management Center

The robust Axis Management Center is an identity management solution that simplifies smart card configuration and administration throughout the organization for logical and physical access. The administrator uses the SafeNet Axis Management Center to:

- Set-up control of password policies for corporate applications.
- Configure smart card policies and select how the smart card will be used.
- Configure and deploy the SafeNet Axis Policy Client for all user desktops.
- Automatically update the Policy Client when Software upgrades are available.

Rapid Deploy Technology™

The true power behind the SafeNet Axis Management Center is found in its Rapid Deploy Technology. Through this technology, Axis learns existing business applications and login procedures. It trains the Policy Client to use smart cards for automated secure access—without requiring any changes to the applications or infrastructure.

Rapid Deploy Technology supports "push" installation of the Policy Client on user desktops via a single central location. After installation, Rapid Deploy Technology automates software and credential updates.

Automated Desktop Management

Through the SafeNet Management Center, administrators can define, build and deploy consistent desktop environments that feature the smart card or token as the cornerstone of user access to all corporate resources. Client software updates take place automatically, without any user action, as defined and controlled by the administrator.

Automated Credential Management

SafeNet Axis gives administrators complete control in defining, enforcing and enabling how each user gets access to applications and resources through passwords stored on the user's smart card. The administrator can establish strong passwords (automatically generated by Axis). It changes them when prompted by corporate applications and transparently "pushes" these passwords to a user's smart card. This push occurs automatically behind-the-scenes when the user logs into the network. And because the user never knows the password (and only needs to remember their own PIN), security is significantly enhanced.

In addition to configuring smart card-based access throughout the company, the Management Center allows administrators to easily define the policies for the smart card itself (minimum PIN lengths, maximum number of re-tries allowed, etc.). This gives them a central location for defining consistent security throughout the organization.

SafeNet Axis Policy Client

Axis Policy Client runs on the user's desktop, connecting the user and all enterprise resources and enforcing smart card policies for corporate access. It provides:

- Control for how the smart card is used and for which applications.
- Automated Single Sign-On to business applications. When users log-in, the Client automatically presents credentials to all applications without additional actions by the user.
- Software "push" installation and updates without any user action. The Axis Policy Client features a light footprint so it installs quickly and easily.
- Built-in logon applications for the smart card—including Windows® logon without using a digital certificate and biometric logon.

Smart Card/Reader (USB Token optional)

For the user, Axis simplifies all access down to a card or token. This one powerful tool stores all passwords and credentials for everything from building access to network log-on and secure access to protected web sites or applications. Axis offers:

- Convenience. When users log-in, they insert the card/token and enter one PIN to unlock the smart card vault. Users then have instant secure access to the network, a VPN, e-mail, protected web sites and business applications.
- Simplicity. Complex corporate passwords may still be used, but as they are stored on the card/token, the user never needs to remember them. These passwords are pushed to users' smart cards/tokens through the Axis Management Center.
- Flexibility. Users also can store their personal passwords on the smart card/token for access to applications or web sites not administered by the company. A user might log-on to an employee benefits web portal to view insurance coverage, or the company's 401(k) provider web site. When users store personal passwords on their smart cards/tokens, they have a personal interest in safeguarding their card/token. Axis promotes familiarity and compliance.

Technical Specifications

Administrator Hardware

Requirements include:

- Pentium or later processor
- Minimum of 16 MB of RAM (32 MB recommended)

One of the following:

- An available serial port, PCMCIA slot, or USB port for a smart card reader
- An available USB port for a USB token

Administrator Software Requirements include:

- Windows 2000 Server, Windows 2000 Professional, Windows 2003 Server, or Windows XP Professional
- Active Directory (if deploying a Policy Client via Group Policy or SMS)
- A network connection to your end-users (if deploying a Policy Client via Group Policy or SMS
- RRAS (for remote access)
- Microsoft CA (for use with PKI)

End-user Hardware Requirements include:

- A Pentium or later processor
- Minimum 16 MB of RAM (32 MB recommended)
- An available serial port, PCMCIA slot, or USB port for a USB smart card or token

End-user Software Requirements include:

- One of the following: Windows XP Professional, Windows 2000 Professional, Windows NT 4.0 Desktop (SP 6a or higher), or Windows 98 SE (requires Active Director Services Interface [ADSI])
- Microsoft Internet Explorer V5.6 or higher

Benefits

SafeNet Borderless Security Credential Management System is versatile and easy to use

Web-based
Easy to roll out enterprise-wide

Fully customizable
Fits into corporate security policies and business rules

Enterprise-controlled credential deployment
Designed to immediately issue credentials at the enterprise, so no need to wait for credential delivery from a service bureau

Secure authentication to server

Can be accessed over a public network

PKI Independent

Digital credential management:
Manage keys, certificates, and data on cards

PIN management:
Reduces calls to your support desk due to forgotten PINs

Broad credential support
Includes support for digital certificates, keys, passwords, biometrics,

Credential Management System

A Web-based Credential Management System for enterprises that are deploying SafeNet cryptographic credentials for identification applications

Web-Based Management

SafeNet Borderless Security Credential Management System is a Web-based digital credential management solution for enterprises — used to issue, manage and support SafeNet cryptographic smart cards and USB tokens for identity-based applications throughout the organization. SafeNet Borderless Security Credential Management System gives enterprise customers a powerful, interoperable and secure system that reduces the cost of deploying and supporting credentials.

Through innovative, policy-based enrollment features, SafeNet Borderless Security Credential Management System significantly reduces the time an enterprise spends issuing and managing smart cards for geographically distributed users. SafeNet Borderless Security Credential Management System makes it easier to perform a wide range of critical digital management activities—everything from requesting or renewing a user's digital credentials to revoking or re-issuing these credentials.

Issuance, Management, and Support Throughout the Enterprise

Deploying and managing smart cards and issuing digital identities can be a huge task without the proper tools. SafeNet Borderless Security Credential Management System removes the complexities associated with deploying smart cards and digital identities, enabling enterprises to quickly leverage the benefits offered by these technologies. SafeNet Borderless Security Credential Management System gives organizations the tools to:

- Issue and electronically personalize cards and tokens—with SafeNet Borderless Security Credential Management System, organizations have a secure web-based system to generate and load digital credentials for central or distributed issuance to many users.
- Manage deployed cards and tokens—SafeNet Borderless Security Credential Management System gives enterprise users the power to easily request and renew their personal digital credentials. A user accesses SafeNet Borderless Security Credential Management System through a published website and receives a list of menu options available according to enterprise policies. Requesting certificates, changing the card pass phrase and renewing certificates etc. are all available through the web-based client interface.
- Support smart card and token users throughout the organization—SafeNet Borderless Security Credential Management System provides help desk tools for supporting smart card and token users in the field, including user card unblocking if the card becomes locked by too many incorrect card log-in attempts, re-issuance for lost or forgotten smart cards and tokens, and revocation of digital credentials to invalidate lost cards.

Easily Integrated

For easy, web-based log-on to SafeNet Borderless Security Credential Management System users and administrators insert their personal smart card or USB token and enter their PIN. Corporate security policy dictates access rights for SafeNet Borderless Security Credential Management System.

Demonstrated Interoperability

SafeNet has earned a strong reputation in the industry for developing smart card technology that strictly adheres to industry standards, allowing for seamless integration with other leading information security products. SafeNet Borderless Security Credential Management System follows in this tradition, featuring broad interoperability with the leading digital credential software solutions.

Enterprise-Controlled Credential Deployment

SafeNet Borderless Security Credential Management System gives enterprises complete control over the deployment of smart cards to users. SafeNet Borderless Security Credential Management System integrates with a company's existing card printing equipment or with other standard card printers to enable immediate deployment of cryptographic smart cards for identity-based applications to users throughout the organization—especially well suited for enterprises that are using SafeNet smart cards as a multi-functional ID badge for both physical and logical access/security.

SafeNet Borderless Security Credential Management System Security

Smart card and digital credential management must maintain the highest level of security. To ensure the integrity of these elements, all management operations are digitally signed, providing a secure and auditable data stream. All critical data transfers are encrypted, and SSL is used to enhance security. Critical fields in the security database are also encrypted.

To access and log-on to SafeNet Borderless Security Credential Management System, users must have their personal smart card, which secures and protects the SafeNet Borderless Security Credential Management System environment.

Technical Specifications

Basic Server Requirements

- Pentium III 800 MHz or equivalent
- 256 MB memory
- 20 GB hard disk
- Windows 2000 Server or Advanced Server
- Microsoft SQL Server 7.0 with Service Pack 3 (or SQL 2000 with Service Pack 2)

Basic Client Requirements

- Intel Pentium 300 MHz or better
- 64 MB memory
- 2 GB hard disk
- Windows 2000 with Service Pack 2 or NT4 with Service Pack 6A
- Microsoft Internet Explorer 5.5 or above

SafeNet Contact Information

SafeNet, Inc
Corporate Headquarters
4690 Millennium Drive
Belcamp, MD 21017
Tel: 410-931-7500
TTY Users: 800-735-2258
Fax: 410-931-7524

www.safenet-inc.com

UK: Rivercourt, 3 Meadows Business Park, Station Approach, Blackwater, Camberley, Surrey, GU17 9AB, UK
Tel: +44 (0) 1276 608 000

www.safenet-inc.com/uk

SafeNet Sales Contact
Toll Free Sales: 1-800-533-3958

Technical Support Contact Information:
Phone: 800-545-6608
eMail: support@safenet-inc.com

Investor Relations
Phone: (443) 327-1239
Email: investorinfo@safenet-inc.com

Public Relations
Maureen Kolb
Phone: (443) 327-1238
Email: mkolb@safenet-inc.com

Export Regulations
Phone: (443) 327-1283
Fax: (443) 327-1216

International Offices
Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538
Japan +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts) +1 978.539.4800
U.S. (Minnesota) +1 952.890.6850
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (San Jose, California) +1 408.452.7651
U.S. (Torrance, California) +1 310.533.8100

Distributors and resellers located worldwide.

www.safenet-inc.com

4690 Millennium Drive, Belcamp, Maryland, 21017 USA
Tel: +1 410.931.7500 or 800.533.3958