# VERSION 3 OVERVIEW

**The SafeNet Security System**

**Version 3 Overview**

SafeNet™

## Abstract

This document provides a description of Information Resource Engineering's SafeNet version 3 products.

SafeNet version 3 products offer a comprehensive centrally managed security solution that enables VPNs to operate at an affordable price. SafeNet is available as an integrated family of products or as a complete, managed VPN security service. Version 3 products provide a full range of Internet security – access control, encryption, user authentication, and message authentication based upon the emerging IPSec industry standards. SafeNet version 3 products include gateway encryptors, client software, smartcards and a management center with an integrated Certificate Authority (CA).

The following sections describe the new version 3 public key functionality as well as the migration from the current version 2.0 secret key SafeNet products to the version 3 public key SafeNet products. Please refer to Appendix A for an introduction to public key technology and concepts or the IPSec White Paper created by the IRE Marketing Department.

## IRE's SafeNet Security System

The Internet, by its nature, is an intricate and freely accessed system that continues to grow at an astounding rate. Through this growth, it has produced a two-edged sword that can provide ease of access in communicating with businesses world-wide but can also give anyone with a computer and a modem free access to any Internet connected Local Area Network (LAN) and to proprietary company information.

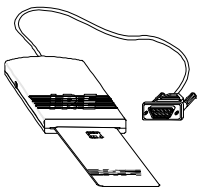
IRE's SafeNet family of products has been developed to meet the computer security needs of corporations and government organizations on the Internet for now and beyond the year 2000. Over the years, IRE has consistently adhered to established security standards. IRE's SafeNet family features both IPSec and FIPS 140-1 approval, the most stringent U.S. government standard for network security products.

The SafeNet Security System allows use of the Internet for sensitive business communications, in place of private and Value-Added Networks. SafeNet also allows users of private TCP/IP networks, most of which have Internet connections, to achieve the level of security necessary to transact sensitive business, including customer information, business plans, personnel data and audit reports, on the network without the use of dedicated, private lines.

SafeNet Version 3 is a comprehensive family of devices, which are easy to use and manage, consisting of:

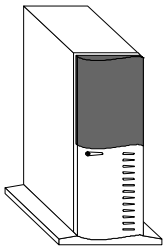
**SafeNet/Soft** – SafeNet/Soft provides the basics of Internet security for your PC. SafeNet/Soft automatically generates a one-time password, encrypts data, and continuously authenticates packets while operating transparently to all application software.

**SafeNet/Smart** – SafeNet/Smart features the same easy to use encryption software as SafeNet/Soft with the added security of token based user authentication through the addition of a smartcard and smartcard reader.

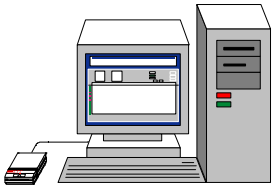


SafeNet™

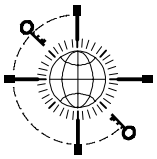
***SafeNet/LAN VPN Encryptor–*** *SafeNet/LAN VPN Encryptor protects direct LAN to Internet connections using DES/TDES encryption technology and packet authentication combined with firewall filtering techniques, creating a Virtual Private Network (VPN). Because SafeNet/LAN is a self-contained unit that responds only to encrypted and authenticated management commands, it cannot be attacked from the network.*



***SafeNet/Firewall*** *–SafeNet/Firewall exceeds industry standards for firewall technology. SafeNet/Firewall protects large area networks, combining a Pentium based proxy server firewall with hardware encryption.*



***SafeNet/Security Center*** *– This Pentium-based workstation is the heart of the SafeNet Security System, providing central security policy management and integrated Certificate Authority services for all SafeNet products. SafeNet/Security Center (SafeNet/Security Center) performs user and device enrollment, Personal Identification Number (PIN) management, event auditing, alarm reports, and network management including configuration downloads. The SafeNet/Security Center can remotely manage one or more SafeNet/Firewalls.*



***SafeNet/Trusted Services*** *–*
*SafeNet/Trusted Services provides security expertise in VPN management. Using SafeNet/Security Centers housed in secure 24x7 facilities, SafeNet/Trusted Services can be contracted to provide comprehensive security management for SafeNet products.*

## SafeNet Version 3.0 System Overview

*SafeNet version 3 introduces an IPSec compliant, public key mode of operation to the SafeNet family of products. In order to ease migration from version 2 SafeNet products:*

- *the version 3 SafeNet/Security Center can enroll and manage both version 2 SafeNet devices and version 3 SafeNet devices,*
- *the version 3 SafeNet/LAN VPN Encryptor can communicate simultaneously with both version 2 SafeNet devices and version 3 SafeNet devices, and*
- *the version 3 clients, SafeNet/Soft and SafeNet/Smart can operate in either a secret key mode of operation (like a 2 client) or in the new IPSec compliant public key mode.*

.

*The SafeNet version 3 system is an IPSec-Plus solution. It is IPSec compliant when used in Public Key mode. The "Plus" is the non-IPSec functionality that SafeNet version 3 products provide in order to enable a comprehensive security policy.*

- *User Authentication – ANSI X9.26 challenge response*
- *Policy set-up, download, and management*
- *Access Control Groups and Checking*

SafeNet™

- Certificate Revocation List (CRL) checking for public key devices
- Key Distribution for secret key devices
- Event Logging

The IPSec standards are still under development in many of the areas listed above including managing and applying security policy, user authentication, and how to request and receive certificates (also known as public key infrastructure or PKI). IRE believes these are important and required elements of an organization's security policy. Therefore we developed the SafeNet version 3 solution with IPSec-Plus functionality so that our customers could realize all the benefits of VPNs immediately, even though some areas of the IPSec standards are still under development.

For applications that require IPSec interoperability of security products, IRE has developed an ICSA certified interoperable client solution, SafeNet Soft-PK. These clients can be deployed within a SafeNet Version 3 environment, but will lack the central management functions described above.

The new public key mode of operation provides full IPSec compliance including support for Internet Key Exchange (IKE, formerly known as ISAKMP/Oakley), DES and TDES encryption algorithms, and MD5 and SHA1 message authentication algorithms. RSA is used for entity authentication, verifying that the ownership of a public key by a SafeNet product or user. In addition, RSA is used for signing product and user public key certificates.

SafeNet version 3 ships with Microsoft Certificate Server integrated onto the SafeNet/Security Center platform to provide all Certificate Authority services including public/private key pair generation, certificate signing, and certificate revocation.

In order to provide the functionality necessary to administer a corporate security policy, SafeNet version 3 products are not interoperable with other IPSec compliant products. Although fully IPSec compliant, SafeNet version 3 acts as a closed system to provide user authentication, access control and certificate checking/revocation functions. These are all areas where the current IPSec standards have not yet reached consensus but are necessary in any system roll-out.

The SafeNet/LAN, SafeNet/Soft, and SafeNet/Smart products have been enhanced to add public key capability to the existing secret key products. These Version 3 products are capable of operating in both a public key and secret key environment. The SafeNet/LAN devices can be configured to operate as either a secret key device only or as both a secret and public key (dual key) device. This allows a SafeNet/LAN to establish secure communications with a mix of public key and secret key remote encryptors. SafeNet/Soft and SafeNet/Smart can be configured to operate as either a public key device or secret key device, but not both simultaneously

The SafeNet/Security Center is capable of servicing both secret key and public key products. Complete support for configuration of IKE parameters for the SafeNet/LAN, SafeNet/Soft and SafeNet/Smart has been added. This includes such parameters as selection of encryption algorithm (DES, TDES), selection of authentication algorithm (DES-MAC, MD5, SHA-1), key life in seconds or kilobytes, and the length of keying

material (IRE group-512 bit, Diffie-Hellman Group 1-768 bit, Diffie-Hellman Group 2-1024 bit).

The SafeNet/Security Center uses Cryptographic Service Messages (CSM's) to perform configuration downloads, event logging, and user authentication. A variant of the secret key X9.17 key delivery mechanism is used when the SafeNet/Security Center is required to check certificate status, access control, or to initiate user authentication. IKE is used to establish secure sessions between devices operating in public key mode. During the process of establishing a secure communications session (Phase I of IKE), the SafeNet/Security Center checks access control, certificate status, and initiates user authentication if required.

For SafeNet/LAN devices, the certificates (and public/private key pair) are associated with the device. For SafeNet/Softs and SafeNet/Smart devices, the certificates are associated with the user. However, since SafeNet/Soft requires the user to be tied to the device, the public key will be indirectly tied to the device. For SafeNet/Smart, the user employs his/her smartcard (which contains user authentication and user certificate and key pair information) and can authenticate using any SafeNet/Smart device.

## Migration From Secret Key

Version 3 of the SafeNet/Security Center enhances the secret key SafeNet/Security Center (version 2). This version 3 SafeNet/Security Center is still capable of servicing secret key devices. The SafeNet/Security Center can distinguish "legacy" secret key devices from new public-key capable devices by their serial numbers. All new public key capable devices have serial numbers of 500,000 and higher. When a Security Officer enters a new device, the SafeNet/Security Center automatically caters the screen to the device's capability based on its serial number. This prevents a Security Officer from configuring an older device for public key operation.

The Version 3 SafeNet/Security Center requires that the Windows NT Server operating system and SQL Server Database be used as opposed to Windows NT Workstation and SQL Workstation Database used on older versions. In addition, there are several applications from the NT Server Option Pack that must be installed in support of Microsoft Certificate Server. As such, upgrades of a version 2 SafeNet/Security Center to a version 3 SafeNet/Security Center involves more than just installation of new SafeNet/Security Center software.

Version 3 SafeNet/Soft and SafeNet/Smart have also been enhanced from the version 2 secret key products and can now operate in either a secret key mode of operation (like a Version 2 client) or in the new IPSec compliant public key mode. The mode of operation (secret key or public key) is controlled by a "key mode" configuration parameter at the SafeNet/Security Center that is included in the configuration smartcard or diskette and in any subsequent configuration downloads. SafeNet/Soft and SafeNet/Smart are capable of being configured for public key operation or secret key operation, but not both simultaneously.

A client configured for public key mode may easily be changed to secret mode by simply changing the key mode parameter. Going the other way is also achievable, but requires more advanced planning in

that upon configuration at the SafeNet/Security Center, the Security Officer must have gone through the public key device configuration screens and issued a user certificate and key pair before switching the device to secret key mode.

A Version 3 client product will appropriately default to secret key operation if installed in a "legacy" secret key SafeNet environment where the key mode configuration parameter is not supported.

In order to support public key in the SafeNet/LAN, the amount of memory (RAM) has been increased and a number of other minor hardware changes have been made. Therefore, a hardware upgrade or swap is required for a Version 2 secret key SafeNet/LAN to be upgraded to a version 3 SafeNet/LAN.

## Communications

In general, communications between the SafeNet/Security Center and the public key devices use the same tried and true mechanisms employed in the existing secret key implementation. For example, event logging continues to operate as it currently does in the secret key implementation but new events have been defined and generated to support the public key devices. Configuration downloads operate the same way as currently performed in the secret key products. This includes the encryption and authentication of configuration data during a configuration download.

A device's or user's private key will not be downloaded or delivered electronically in any way. It is always written to the smartcard for SafeNet/LAN and SafeNet/Smart or diskette for SafeNet/Soft. Since the certificate is associated with the user data, it can't be downloaded and must be written to the smartcard (diskette) at the SafeNet/Security Center . The CA certificate is part of the device configuration data, and is included in the configuration downloads and configuration smartcards (diskettes). (See section 5 for details.)

The user authentication process continues to use the X9.26 sequence that is used in version 2 SafeNet products and continues to use the user keys on the smartcard (or the "virtual smartcard" on the PC hard drive for SafeNet/Soft). It is not based on the user certificate or the key pair. Like version 2 products, the need for the user authentication process is still based on the configuration setting of the SafeNet/LAN as required, preferred, or not required.
In the version 3 design, the receiving encryptor always contacts the SafeNet/Security Center prior to establishing a secure session. Contacting the SafeNet/Security Center serves three purposes:

1. To determine if user authentication is required (if required, user authentication will then commence)
2. To check access control (based on device serial number).
3. To check the certificate status (i.e. is it revoked?).

## Secure Session Establishment

The public key devices use IKE to establish a security association and session key. During IKE negotiations, the devices contact the SafeNet/Security Center to determine whether or not the session can be established. As described previously, the SafeNet/Security Center checks certificate status, access control, and/or initiates user authentication. Once the SafeNet/Security Center "approves" the session establishment, it sends a response back to the devices. In order to check certificate status, a device sends the serial number for both its certificate and the peer certificate.

The mechanism for contacting the SafeNet/Security Center for "approval" is based on Cryptographic Service Messages (CSMs). The certificate serial numbers are appended to the CSMs, as appropriate. The SafeNet/Security Center and encryptors differentiate public key CSMs from secret key CSMs by the embedded certificate serial numbers and the inclusion or exclusion of a key management parameter. When the SafeNet/Security Center receives a public key request, it checks device-to-device access control and initiates User Authentication if appropriate. The SafeNet/Security Center also uses the certificate serial numbers in the CSM to check whether or not the certificates have been revoked, suspended, or expired. If the SafeNet/Security Center approves secure session establishment, it sends notification to the device. Once the device receives the positive acknowledgment, it proceeds with establishment of the secure session with the peer public key device.

## Certificate Authority

Microsoft Certificate Server resides on the same PC as the SafeNet/Security Center and provides all Certificate Authority services. Microsoft Certificate Server is a separate Microsoft product that ships as part of Windows NT Option Pack and is included by IRE with the purchase of a SafeNet/Security Center. The SafeNet/Security Center application contains functionality to send certificate requests to the CA service and receive signed certificates from the CA.

The private key of the CA is securely stored (using CAPI) in the registry. The Microsoft Certificate Server contains instructions on how to backup the Certificate Server and its key pair. There is an option in the Certificate Server installation program to use the existing keys and certificate, rather than generating a new key pair and self signed certificate, in case the CA needs to be reinstalled. The SafeNet/Security Center requests the CA certificate from the CA and stores it in the database.

The CA is configured to only accept certificate requests from the SafeNet/Security Center. It will not issue certificates directly to other clients (e.g. a Web browser or other vendors' products).

Version 1.0 of the Microsoft Certificate Server works exclusively with the Microsoft Base CSP and thus only signs with a 512 bit RSA key. Future versions of Microsoft Certificate Server are expected to allow the use of any CSP. In turn, we expect the ability to support 768 bit and 1024 bit signatures through the inclusion of the IRE CSP in future releases of the SafeNet/Security Center.

SafeNet™

## Certificates and Smartcards

Advanced smartcards with 8K of memory are used for public key functionality. New configuration and user parameters for public key devices have been added to the existing smartcard data structure while retaining backward compatibility with existing secret key devices

The CA certificate (which includes the CA public key) is included in the device configuration data, not with the user data (which has the user private key and certificate). This provides some additional security benefits:

- The devices are able to provide some limited local authentication by checking the CA signature on the user certificate.
- The CA certificate can be changed by downloading the new certificate to the device from the SafeNet/Security Center.
- This prevents the scenario where someone could replace the smartcards of two users with fake cards. These would have bogus certificates signed by a fake CA along with a fake CA public key. Having the device verify the user certificate with its CA certificate prevents this attack.

For SafeNet/LAN the public key information (private key and certificate) is included in a new SafeNet/LAN smartcard. The version 3 implementation allows only one user smartcard per SafeNet/LAN device, effectively associating the private key and the certificate with the device itself. This is accomplished by the SafeNet/Security Center creating a SafeNet/LAN smartcard with a user ID equal to "LAN <device serial number>". The SafeNet/LAN verifies that the user ID matches the device serial number before the card is used. For SafeNet/Soft and SafeNet/Smart, the public key information is associated with the user, not the device. This means that it is stored on a user smartcard for SafeNet/Smart, or in the user segment of the diskette for SafeNet/Soft. As is currently done in the version 2.0 SafeNet products, the user ID for SafeNet/Smart and SafeNet/Soft is not tied to the device serial number.

Public/private key pair generation is performed in software at the SafeNet/Security Center (using Crypto API, or CAPI). A PKCS#10 certificate request (includes the public key and is signed with the private key) is generated by the SafeNet/Security Center and sent to the CA (which is a service running on the same PC). The CA returns a certificate that is signed by the CA's private key. The SafeNet/Security Center writes the user private key and the user certificate to the user smartcard (or diskette for SafeNet/Soft). The key pair is not generated on the smartcard itself, but within the SafeNet/Security Center using CAPI. The SafeNet/Security Center writes the CA certificate to the configuration smartcard (or diskette). The configuration data (which has the CA certificate) and the user data (which has the private key and user certificate) can be written to a single combination smartcard (or diskette).

Note that the private keys are not stored in the SafeNet/Security Center database or registry. Once a private key is written to a smartcard (diskette), it is deleted from the SafeNet/Security Center. Similarly, if a key pair is generated but not written to a smartcard (diskette), the key pair and certificate are deleted from the SafeNet/Security Center when the device or user screen is exited.

Public key X.509 version 3 certificates are used. Currently, Microsoft Certificate Server includes the Authority Key Identifier extension in user certificates and the Key Usage, Basic Constraints, and Subject Key Identifier extensions in the self-signed CA certificate (also known as. root certificate). Certificates do not contain any additional certificate extensions.

The SafeNet/Security Center includes a utility that enables a Security Officer to retrieve certificates from the SafeNet/Security Center database and display their contents and status to the Security Officer.

A Certificate Revocation List (CRL) is not published nor downloaded to the devices, rather a certificate status is maintained by the SafeNet/Security Center Because devices are required to come to the SafeNet/Security Center for authorization, certificates are checked for validity then.

## Certificate Expiration

The CA certificate and the user certificates contain expiration dates. The CA certificate is typically valid for a period of five years. The validity period of user certificates is controlled by the SafeNet/Security Center and ranges from 1 – 12 months from the date of issue.

Certificate renewal is not supported by the SafeNet/Security Center. (Within the IPSec standards bodies, there is no agreement upon the concept of certificate renewal.) When a certificate expires, there is no mechanism for "re-certifying" that public/private key pair. A new key pair must be generated along with a new certificate and delivered to the device via smartcard or diskette.

SafeNet/Security Center Version 3 features a Certificate Expiration Log utility that allows the Security Officer to examine all currently valid certificates and list them in order of when they will expire. Using this mechanism, the Security Officer can ensure that certificates don't expire before new certificates are issued.

There will always be some delay between when a new user certificate is issued and when the user actually starts using the new certificate. During this period, the user continues to use his/her old certificate, assuming it hasn't expired or been revoked. Therefore, the old certificate is maintained in the SafeNet/Security Center until the new certificate is activated by the user. In this way the SafeNet/Security Center can still check revocation status of the old certificate while it is still being used.

# Appendix A

# Introduction to Public Key Technology and Concepts

### About Public Key Encryption

There are two major types of encryption systems: secret key (also called symmetric key) and public key. In each system, data is encrypted using an algorithm, such as DES, and by using a key that is shared by the two parties. The difference between secret key and public key systems is in the way that the shared key is obtained.

Public key systems allow you to communicate securely with another party without advanced awareness of each other. It is based on key pairs- literally a private key, which each user has, and a public key that can be distributed to anyone by a Certificate Authority or directory server.

Unlike secret key technology, public key technology does not require a real-time, online, centralized key management system to distribute keys for each communication session. Because public key can be implemented on a peer-to-peer basis without requiring centralized key distribution, it is infinitely scaleable. Further, since each individual control his or her own private key, open systems can be implemented securely. This allows multiple VPN users to communicate safely across a public network. Public key is the technology that promises to be the 21st century standard.

### Digital Certificates and Certificate Authorities

Another component of public key technology is a digital certificate. To be able to trust that a communicating party is who they say they are, a "trusted" third party, called the Certificate Authority (CA), is required. A CA issues a digital certificate, which is an electronic file that is "signed" by the issuing CA organization, based on the user having provided some proof of identification. This digital certificate can then be bound to the associated user's public key, providing the recipient of the user's message assurance of identity.

### Internet Key Exchange

Internet Key Exchange (IKE) defines how communicating parties establish shared keys to be used for data encryption and message authentication.

There are two phases:

**Phase 1 - Authentication.** During Phase 1, communicating parties reveal their identities and negotiate how they will secure Phase 2 communications. There are two varieties of Phase 1: Main Mode (MM) and Aggressive Mode. Main Mode provides identity protection; identities are not revealed until secure communications have been established. In Aggressive Mode, identities are revealed before secure communications have been established, reducing the number of Phase 1 steps. Authentication is accomplished through the use of digital signatures and identity certificates or pre-shared keys (see below).

### Pre-Shared Keys

In addition to using digital signatures and certificates, IPSec compliant products must support the use of pre-shared keys for authentication. This means that the two communicating parties have agreed upon an authentication key prior to communications. A digital certificate is not necessary when using a pre-shared key. Authentication of the other party during phase 1is based on the fact that they have the same pre-shared key.

**Phase 2 - Key Exchange.** During Phase 2, also known as Quick Mode (QM), the parties negotiate the encryption and message authentication algorithms and develop the necessary shared keys to be used for secure communications. Phase 2 communications are secured as negotiated during Phase 1.

The end result is a security association between the two parties consisting of an encryption algorithm, a message authentication algorithm, and the associated data encryption keys and message authentication keys needed to secure communications.