SafeNet Security Policy

Abstract

This document provides a high level description of the *IRE* SafeNet products. Also included is a description of the security services, key management system, and authorized operator roles.

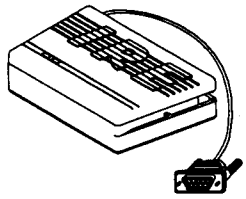
1.0 IRE's SafeNet Security System

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 connected Local Area Networks (LANs) and to company information. The SafeNet family of products have been developed to meet the computer security needs of corporations and government organizations on the Internet for now and beyond the year 2000.

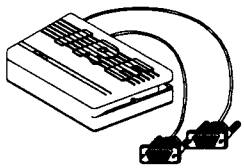
The SafeNet Security System allows you to use the Internet for your most sensitive business communications, in place of private and Value-Added Networks. It also allows users of private TCP/IP networks, most of which have Internet connections, to achieve the level of security necessary to transact sensitive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

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

- **SafeNet/Dial Secure Modem** – The portable, pocket-sized SafeNet/Dial Secure Modem protects dial connections that are made from remote users' locations. It includes an internal V.34 modem, supporting terminal-to-modem communication rates up to 115.2 Kbps and modem connections rates up to 28.8 Kbps on both secure and non-secure systems. The SafeNet/Dial is designed to provide data encryption, user authentication, and packet authentication security services. It is available for both desk-top and notebook applications.

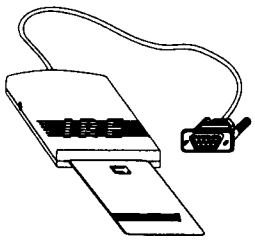


- **SafeNet/Dial-R Encryptor** – To meet the needs of users who already have modems, the SafeNet/Dial-R Encryptor incorporates all the security features of a SafeNet/Dial Secure Modem—but without an internal modem. It establishes a security barrier between a user's PC and an external modem, protecting dial connections and providing data encryption, user authentication, and packet authentication on both secure and open systems. It includes power cords that draw power from the keyboard port of either notebook or desk-top computers.

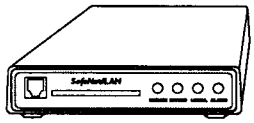


- **SafeNet/Soft** – This software product adds cryptographic security to your personal computer. Using software running on your PC hard drive, it processes user PINs and one-time passwords, produces authentication packets, and encrypts incoming and outgoing information between secure sites on a case-by-case basis. SafeNet/Soft provides you with the basics of Internet security.

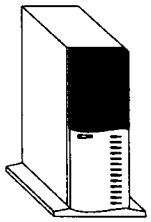
- **SafeNet/Smartcard** – A step up from SafeNet/Soft, the SafeNet/Smartcard product includes a smartcard reader and software programs that run on your personal computer. The smartcard requires an additional level of input for authorized use. SafeNet/Smartcard continues to provide the same data encryption, user authentication, and packet authentication as *IRE*'s other SafeNet remote access products.



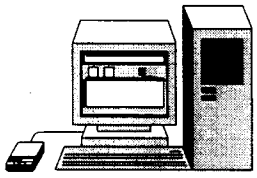
- **SafeNet/LAN VPN Encryptor**– The SafeNet/LAN protects direct LAN to Internet connections using encryption technology and packet authentication combined with firewall filtering techniques, creating a Virtual Private Network (VPN). Unlike conventional firewall products, because the SafeNet/LAN is a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



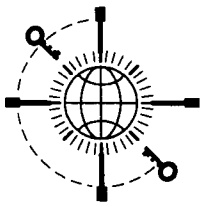
- **SafeNet/Firewall** – The SafeNet/ Firewall product exceeds industry standards for firewall technology. The SafeNet/Firewall protects large area networks, combining a Pentium proxy server firewall with VPN Encryptor hardware.



- **SafeNet/Security Center** – This Pentium-based workstation is the heart of the SafeNet Security System, providing central management for all SafeNet products. The SafeNet/Security Center performs key management, registrations, user and device enrollment, Personal Identification Number (PIN) management, event auditing, alarm reports, and network management including parameter downloads. The S/SC can remotely manage one or more SafeNet/Firewalls. It is designed to support a broad range of security products operating on multiple networks using a combination of key management technologies.



- **SafeNet Trusted Services Corp** – SafeNet Trusted Services provides security expertise in VPN management. Using SafeNet/Security Centers (see above) that are housed in secure facilities, SafeNet Trust can be contracted to provide key management for clients' SafeNet products.



A typical SafeNet Security System configuration is shown in Figure 1-1.

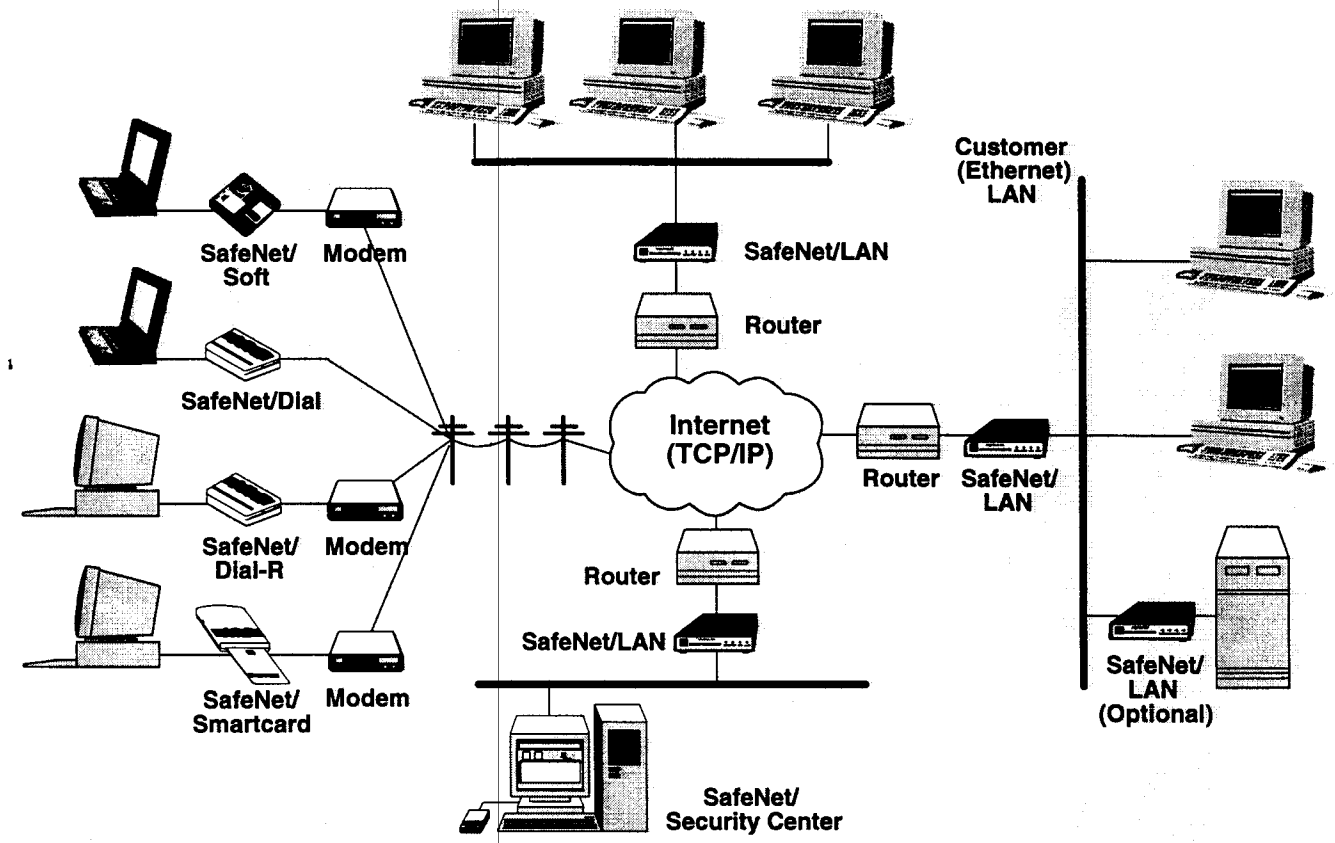


Figure 1-1. Typical SafeNet Security System Configuration

2.0 Comprehensive Security Services

To address threats to data communications, *IRE*'s SafeNet products broadly apply cryptography to authenticate users, keep data private, strengthen firewall functions, authenticate packets, and prevent spoofing. Once SafeNet products are configured, security services are virtually transparent to the user, the applications, and the Internet. Note that while the security services described in this section are the primary features of the SafeNet products, an overview of all of the available services is contained in section 4 of this document.

The SafeNet family of products provide:

- *Data Encryption.* Encryption, implemented in a standards-compliant fashion, protects the privacy of sensitive transmitted data by scrambling and rendering the data unreadable. It assures that data cannot be viewed or meaningfully altered by monitoring devices on the network.
- *User Authentication.* Remote users are authenticated using a complex, "one-time" password that is generated for each communication session from their Personal Identification Number (PIN). This prevents unauthorized access by hackers with stolen passwords. Remote encryption devices (SafeNet/Dial, SafeNet/Dial-R, SafeNet/Soft, or SafeNet/Smartcard) generate the password; SafeNet/Security Center authenticates the remote user.
- *Packet Authentication.* Cryptographic authentication of header, counter, and encrypted information on all secure packets prevents hacker attacks using IP address and header spoofing.
- *Address and Socket Filtering.* If permitted by your organizational security policy, address and socket filtering allow you to manage access by unsecured locations.
- *Tunnel Processing.* Tunnel processing pertains to the recognition of private IP addresses behind a publicly-addressed firewall in a Virtual Private Network (VPN) environment. Tunnel processing features within the SafeNet products permit the

encrypted transfer and conversion of the private IP addresses to enable messages to be delivered to the proper party behind the firewall.

Each of these are discussed further in the following sections.

2.1 Data Encryption

Encryption for the SafeNet System is introduced at the packet level, so that data flows across complex networks and is fully compatible with TCP/IP protocol. The encryption process includes three basic steps—encryption, transmission, and decryption—all of which are accomplished without any user action.

- Prior to transmission, data is encrypted (scrambled) by performing a mathematical calculation using a secret or private number (depending upon the key management techniques employed) called a key.
- During transmission, data is completely meaningless to any viewer.
- At the receiving end of communication, data is decrypted by performing another calculation. Secret key techniques use the same key as used by the sender; public key techniques use a public/private key combination.

Access to an encrypted network may occur only if the remote location has an authorized remote product, such as the SafeNet/Dial, and is explicitly authorized at the SafeNet/Security Center.

2.1.1 The Data Encryption Standard (DES)

The mathematical algorithm which *IRE* uses to implement encryption is set forth in ANSI standard X3.92, the Data Encryption Standard (DES). DES is the preferred encryption algorithm for private industry and government applications. This is a national standard, originally developed by IBM and then certified by the National Institute of Standards and Technology (NIST) for use in commercial and sensitive-unclassified government applications. DES is approved to export for use in financial applications and by U.S. corporations and their subsidiaries.

2.1.2 The ATLAS Algorithm

IRE's SafeNet products optionally employ the ATLAS algorithm for data encryption. The ATLAS algorithm is an *IRE* proprietary algorithm. Like DES, ATLAS relies on individual private keys to protect data from unauthorized decryption. ATLAS devices employ a Master Key of 40 bits. ATLAS is approved by the U.S. Government to export for use in non-financial type applications including commercial and government.

2.2 User Authentication

IRE's SafeNet Security System performs user authentication in accordance with ANSI Standard X9.26. User authentication assures that only authorized individuals are permitted to access the secured destination. The basis of user authentication is two-part: you are the sole user of the authorized remote product, and you are the only one who knows your Personal Identification Number (PIN). Similar to banking with an Automated Teller Machine, you must enter your PIN at the beginning of the communication session. After that, the secure session automatically and transparently takes place.

The process of user authentication begins when the user of the remote encryptor (SafeNet/Dial, SafeNet/Dial-R, SafeNet/Soft, or SafeNet/Smartcard) accesses the SafeNet PIN Entry Program, enters a PIN, and places a call to the Internet access server. The SafeNet remote device sends a message to a SafeNet/LAN to begin security services. This message is relayed by the SafeNet/LAN to the SafeNet/Security Center (S/SC). The S/SC verifies that the products are enrolled in its database and that they are to perform user authentication. If so, the S/SC issues a random number that is used as a challenge to the remote encryptor.

The remote encryptor performs a calculation on the random number challenge and the user-entered PIN, encrypting the result under the secret User Key. This creates a one-time password that is sent to the S/SC. The S/SC performs the same calculation. If the two results match, the user is confirmed to be authorized. This powerful form of password protection automatically transforms a user's PIN into a new random password for each communication session. In this way the password is used only one time so that, even if a hacker captures it, it is immediately obsolete.

2.3 Packet Authentication

Packet Authentication assures that the content of a message has been unaltered in transmission across a network. In Internet applications, each TCP/IP packet represents a separate "message." To each encrypted packet, SafeNet products automatically add a "security header." This protects the data and contains a security Message Authentication Code (MAC), calculated using DES encryption. The receiving SafeNet encryptor validates the MAC to make sure the data has not been altered. Because of this cryptographic protection, intruders cannot "spoof" IP addresses and gain access to resources attached to the Internet or the private TCP/IP network, a common form of attack. Socket services and user data are also protected against alteration.

2.4 Address Filtering

Filtering allows SafeNet products to be configured to support your organization's security policy and application. SafeNet products can be set up to support only secure communication or a combination of secure and unsecured transmissions based upon the network address and Internet service set for your system.

2.5 Tunnel Processing

Tunnel processing may be required for a SafeNet encryptor that is in a private network or behind a firewall to communicate outside the VPN. In these environments the firewall or VPN has a known, public IP address, but the IP addresses of the devices protected by it are anonymous. Tunnel processing encrypts the private IP addresses for transport and then deciphers them through a separate process in order to be received by the proper party.

3.0 Key Management

The SafeNet product family supports ANSI X9.17 secret key management as required by banking and government standards.Central to this key management strategy is the SafeNet/Security Center, which acts as a Key Distribution Center. Recognizing the current evolution in key management standards and organizational requirements, *IRE* has engineered the products with an upgrade path from secret key to certificate-based, public key management.

Key Management in *IRE*'s SafeNet product line conforms to the basic principles of cryptographic protection:

- Each communication session is encrypted under a new randomly-generated key that is erased from Random Access Memory (RAM) at call termination or key expiration.
- Keys cannot be read out of key storage once installed in a security device.
- Each remote device stores a unique key (Master Key) and deviceserial number in non-volatile memory. This key serves as an encrypted identification for a device and allows Security Officers to deny access to the network for a specific device.
- Master Keys can be automatically-generated random numbers.
- Session Keys are never exchanged in clear text, but only safely encrypted under another key.
- The key exchange process operates according to ANSI Standard X9.17.

3.1 Key Types

Within the SafeNet Security System there are three types of electronic keys that can be changed through either random generation or manually as specified by ANSI X9.17. These encryption keys are used for secure key delivery, exchange, storage and management.

The three levels of keys are Storage Key, Master Key and Session Key. These keys are defined as follows:

- *Storage Key – KM0*
  A manually-entered or randomly-generated DES key used to encrypt Master Keys stored electronically in the SafeNet/Security Center. KM0 is used to encrypt/decrypt Master Keys and other critical security parameters. In accordance with ANSI X9.17, the Storage Key must be changed manually. KM0 is stored in the cryptographic module (24J board) that is within the S/SC.
- *Master Key – KK*
  A manually-delivered DES key used to encrypt and decrypt Session Keys exchanged between devices establishing communications with each other. Master Keys are located within a tamper-proof enclosure at individual devices throughout the network. The Master Keys for all devices are also stored in the S/SC after being DES encrypted under KM0.
- *Session Key – KD*
  An electronically-generated and delivered DES key used to encrypt/decrypt or authenticate user data during

communications sessions. The S/SC, acting as a Key Distribution Center, automatically generates and delivers (in accordance with ANSI X9.17) a new Session Key for each communication session between SafeNet encryptor pairs.

3.2 Key Distribution

As the Key Distribution Center, the S/SC is the fundamental component in the generation, storage, and distribution of both Master Keys and Session Keys. Master Keys are generated and manually distributed for each SafeNet encryptor. The Master Keys are used to encrypt/decrypt the Session Keys which are distributed electronically in accordance with ANSI X9.17. All data exchanged during a secure session between two devices is encrypted and authenticated by a Session Key.

The Master Key for each SafeNet encryptor is generated (manually or randomly) by the S/SC. Once the Master Key for a device is generated, it is DES encrypted under KM0 and stored at the S/SC in a database. The Master Key is also DES encrypted under a configuration PIN and written to a configuration smartcard (or diskette for SafeNet/Soft). The configuration smartcard and associated PIN are manually distributed (separately) to the Security Officer responsible for configuring the SafeNet encryptor. At the remote encryptor, the Security Officer inserts the smartcard into the encryptor and runs a configuration utility which prompts for the PIN. If the PIN is verified to be correct, the device reads the configuration smartcard, decrypts the Master Key, and writes it to its non-volatile memory.

Distribution of Session Keys is performed by the S/SC. When the S/SC receives a key request from an authorized pair of encryptors, it generates a random Session Key for data encryption and authentication. As described in ANSI X9.17, Session Keys are encrypted separately by the Master Key of both the requesting device and the peer device. The encrypted Session Keys are then sent electronically to the two SafeNet encryptors. Each encryptor uses its own Master Key to decrypt the Session Keys. The Session Key is then used by each device to encrypt/decrypt and authenticate all data being exchanged in the secure communications session.

3.3 Key Storage

The Storage Key (KM0) is only resident in the S/SC. The key is stored in a separate tamper-proof cryptographic board which is installed in the S/SC workstation. Once entered, the value of KM0 cannot be displayed by the Security Officer operating the S/SC.

Encryptor Master Keys are stored in both the S/SC and the individual encryptors. At the S/SC, each device Master Key is DES encrypted under KM0 and stored in a database indexed by the device serial number. Once entered, the Master Keys cannot be displayed by the Security Officer operating the S/SC. Once the Master Key has been loaded into the encryptor, it is stored in non-volatile memory. The Master Key is used internally by the encryptor and cannot be read out of the device nor displayed to the device operator.

Session Keys are randomly generated by the S/SC and then electronically distributed to the encryption devices. The S/SC does not retain the Session Keys once they are distributed. The encrypted Session Keys are received by the devices and then decrypted with the device's Master Key. Each Session Key is stored in RAM within the encryptor until the communications session is terminated or the key expires, at which time the Session Key is erased.

3.4 User Authentication Keys

The S/SC generates User Keys in support of ANSI X9.26 User Authentication procedures. Similar to encryptor Master Keys, the User Keys can be generated manually or randomly by the S/SC. Once the User Key is generated, it is DES encrypted under KM0 and stored in an S/SC database. The User Key is also written to a user authentication smartcard (or diskette for SafeNet/Soft). The user authentication smartcard and associated user PIN are manually distributed (separately) to the remote encryptor user. As described in Section 2.2, the random challenge - user PIN combination is encrypted under the User Key as part of the ANSI X9.26 User Authentication process.

4.0 Roles and Services

A secure network with the latest technology is only effective if the security policies and procedures are enforced. An integral part of the development of a company-specific security policy is the definition of the operator roles and the authorized services provided by the encryption devices. *IRE* SafeNet products have been developed with specific roles and services defined to allow easy incorporation into a company-specific security policy.

4.1 SafeNet/Security Center

The SafeNet/Security Center is the heart of the SafeNet Security System, providing central management for all SafeNet products. The SafeNet/Security Center performs key management, registrations, user and device enrollment, Personal Identification Number (PIN) management, event auditing, alarm reports, and network management including parameter downloads. The S/SC can remotely manage one or more SafeNet/Firewalls.

Serious consideration must be used in setting up user access to the S/SC. It is important that the individuals provided access to this system are trustworthy, since the information they have access to, in varying degrees, can affect the credibility of the entire secure network. There are six levels of access privileges defined in the S/SC—from the Security Administrator with access to all areas of the workstation, to the Maintenance personnel with limited access to only the backup and archive features. The six distinct levels of access to the S/SC are summarized below.

- *Security Administrator*
  This is the highest level of access available to users of the system. This level is capable of establishing access levels for security personnel, modifying critical configuration settings, authorizing network devices, administering access controls, setup of the event log backups, reviewing and clearing alert messages as well as accessing diagnostic messages.
- *System Administrator*
  The System Administrator has essentially the same capabilities of the Security Administrator, with the exception of revising critical configurations, and can only view the listing of all security personnel. The System Administrator is capable of viewing and modifying network databases; modifying related configuration settings; backing up and restoring all databases; maintaining access control; backing up, archiving, clearing, and viewing the Event Log; acknowledging alerts; and viewing diagnostic messages.
- *Network Administrator*
  At the third highest level, the Network Administrator may view and modify network databases, view configuration settings, view Security Officer access; administer backup databases, access control and S/SC sites; archive and view the Event Log, acknowledge alerts, and view diagnostic messages.
- *Network Monitor*
  The Network Monitor level is provided to personnel who will routinely operate the system, viewing diagnostics, acknowledging alerts, and backing up the databases.
- *Event Monitor*
  Event monitors are only capable of viewing the Event Log.
- *Maintenance*
  This level is used in situations where employees other than the security personnel and administrators would be backing up the S/SC computer databases, as well as archiving and backing up the Event Log.

4.2 SafeNet Encryption Devices

Services provided by the encryption devices can be broken into two categories: services that involve the transfer of data and services related to operation of the encryptor. Services included in the data transfer category are secure data, bypass data, discard data, and user authentication. The encryptor configuration, self-test, and status indication services are all related to operation of the encryptor. While all these services are provided by the encryptors, the primary purpose of the devices is the transfer of secure data. As such, Section 2 of this document describes in detail the elements that make up the secure data service: data encryption, user authentication, packet authentication, address and socket filtering, and tunnel processing.

The remote encryptors support four different roles: security officer, user with authentication, user without authentication, and remote manager. The S/LAN encryptor supports the security officer and remote manager roles. A summary of the different roles follows.

- *Security Officer*
  The security officer is responsible for configuring the encryptor. This can be done using a smartcard and associated PIN, or through the local interface.

- *User With Authentication*
  There are two different user roles that are supported by the remote encryptors. The first role, user with authentication, requires the user to enter an alphanumeric PIN (password) and smartcard for authentication before secure data services are provided.
- *User Without Authentication*
  The second user role does not require identity-based authentication before authorized services are provided to the operator. This role is used by remote encryptor operators when they transfer data with a peer device that does not require user authentication for access.
- *Remote Manager*
  The remote manager role is filled by the SafeNet/Security Center (S/SC). The S/SC provides configuration downloads and key management. The S/SC is capable of preventing the devices from performing secure communications.

There is no *maintenance role* authorized for the SafeNet encryptors. A Security Officer with access to the encryptor configuration parameters may provide assistance with troubleshooting. If, after contacting *IRE* Client Support, the problem is not resolved, the encryptor must be returned to the manufacturing facility for repair.

Appendix A: SafeNet/LAN Tamper Evidence

One of the many benefits of the SafeNet/LAN encryptor is its high level of physical security. Although the SafeNet/LAN encryptor is enclosed in a physically secure case, the rear panel can be removed. Under normal conditions removal of the rear panel will result in zeroization of the critical security parameters. Whenever it is suspected that the S/LAN has been tampered with in an attempt to circumvent its physical security features (i.e. the SafeNet/LAN is in an alarm state), the following should be checked for tamper evidence:

- Whether the paint on the case (especially the rear panel) has been scratched or shows similar signs of an unauthorized attempt to penetrate the enclosure.
- Whether the silicone coating on the switch is present and intact (without any large holes).
- Whether the metal cup on the inside of the rear panel is present and intact so that there will be no gap between the panel and the switch when the module is closed.

The paint can be visually inspected without opening the device. The other two areas may be checked by opening the rear panel and removing the S/LAN cover. If the silicone coating and the metal cup have not been tampered with, then the S/LAN can be safely reconfigured. Otherwise, the silicone coating and the metal cup should be properly fixed before reconfiguring the S/LAN.