The SafeNet Security System

TECHNICAL WHITE PAPER

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.

SafeNet™

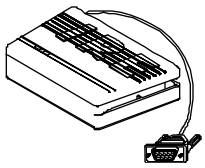
IRE SafeNet Security System

The Internet, by its nature, is an intricate and freely accessed system that continues to grow at an astounding rate. This growth 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. The IRE 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

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.

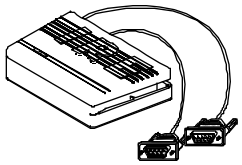
SafeNet is a comprehensive family of devices, which are easy to use and manage, consisting of:

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 and a hardware encryption module. SafeNet/Dial is designed to provide data encryption, user authentication, and packet authentication security services. SafeNet/Dial allows users to secure communications with multiple host sites using separate keys for each relationship

SafeNet/Dial-R Encryptor



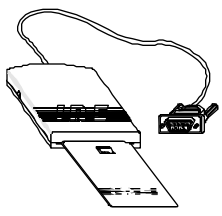
To meet the needs of users, who already have modems, the SafeNet/Dial-R Encryptor incorporates all the security features of a SafeNet/Dial Secure Modem—but without an internal modem. It establishes a security barrier between a user's PC and an external modem.

SafeNet/Soft

SafeNet/Soft provides the basics of Internet security for your PC. SafeNet/Soft incorporates all the security features of a SafeNet/Dial in a simple easy to use software utility.

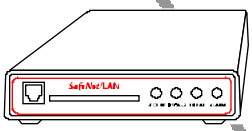
SafeNet/Smart

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™

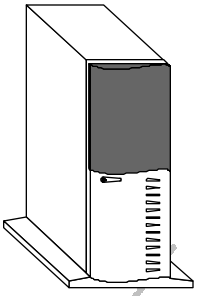
SafeNet/LAN VPN Encryptor



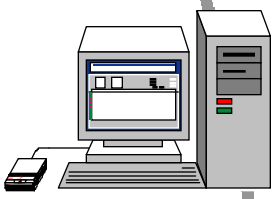
SafeNet/LAN VPN Encryptor protects direct LAN to Internet connections using encryption technology and packet authentication combined with firewall filtering techniques, creating a Virtual Private Network (VPN). Because SafeNet/LAN is a self-contained unit that responds only to encrypted and authenticated 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 T-1 speed hardware encryption.



SafeNet/Security Center



This Pentium-based workstation is the heart of the SafeNet Security System, providing central management for all SafeNet products. SafeNet/Security Center (S/SC) performs key management, 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.

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 key management for SafeNet products.

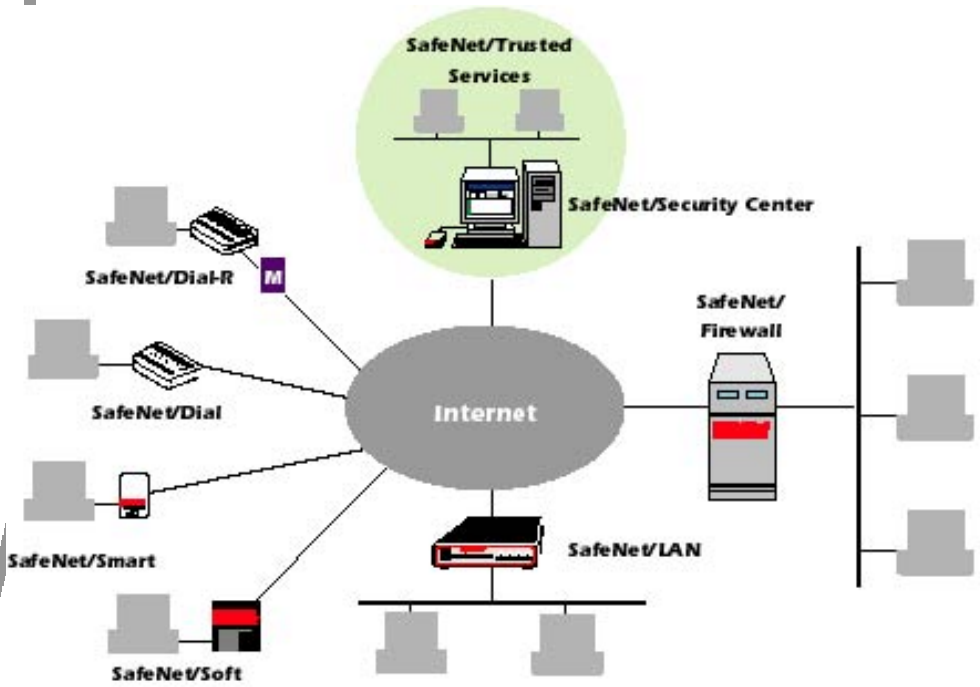


Figure 1
Typical SafeNet Security System Configuration

SafeNet™

Comprehensive Security Services

To address threats to data communications, IRE 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.

The SafeNet family of products provides:

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 the user's 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 VPN environment. Tunnel processing features within 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.

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) through performance of 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 through performance of 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 a secure network occurs only if the remote location has an authorized remote product, such as the SafeNet/Dial, and is explicitly authorized at the SafeNet/Security Center.

SafeNet™

The Data Encryption Standard

The mathematical algorithm that 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. DES 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 for export for use in financial applications and for use by U.S. corporations and their subsidiaries.

The Strength of DES

There are many types of encryption algorithms. DES is a block cipher that encrypts data in 64-bit blocks. A 64-bit block of clear text goes in one end of the algorithm and a 64-bit block of encrypted text comes out the other end. The key length is 56 bits. The key can be any 56-bit number and can be changed at any time.

The building block of DES is a single combination of the two basic techniques of encryption: confusion (substitution) and diffusion (permutation). Each iteration of substitution and permutation based on the key is known as a "round". DES employs 16 rounds. DES uses only standard arithmetic and logical operations on numbers of at most 64 bits and was therefore easily implemented in late 1970s hardware technology.

There has been more scrutiny of DES than any other encryption algorithm in history. There has been much speculation about the key-length, number of rounds, and design of the substitution algorithm. Over the years new methods of cryptanalysis, the science of code breaking, have been developed. DES has held up remarkably well against Differential Cryptanalysis and Related Key Cryptanalysis techniques that were not publicized until the 1990s. It appears that the designers of DES knew something about these types of cryptanalysis well before there was public knowledge of such methods, as the DES key length, number of rounds, and design of the substitution algorithm have proven to work well against these new methods of cryptananlysis.

To discover a key by exhaustive search requires trying all 2^56 possible keys. 2^56 is an enormous number. A computer or group of computers trying 1 million keys every second, 24 hours a day, seven days a week would take 2283 years, 4 months and 12 days to discover the key. Even if 100 million keys per second were tried, it would take almost 23 years to discover the key. Given the time, resources, and money required, it is not practical to develop a DES cracking machine, particularly if the value of the information to be obtained from discovery of the encryption key is considered. Since SafeNet products change the key according to security policy for established LAN to LAN sessions and for every session involving remote client access, a compromised key is only useful one time.

SafeNet™

User Authentication

The 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 (something you have) and you are the only one who knows your user PIN (something you know). Similar to banking with an Automated Teller Machine, the user enters a PIN at the beginning of the communication session. After that, the secure session automatically and transparentl 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 S/SC. The S/SC verifies that the products are enrolled in its database and that they are to perform user authentication. The S/SC then 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 authenticated and permitted access. 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.

Packet Authentication

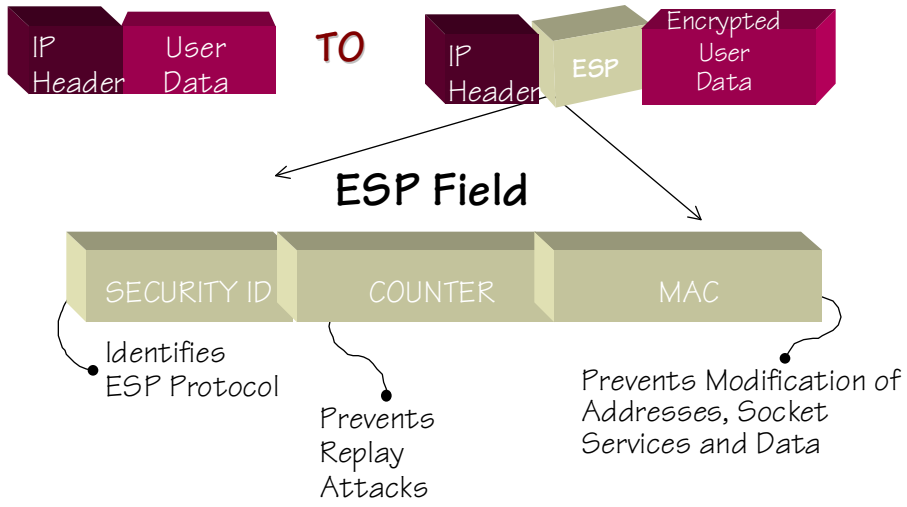
When transmitting sensitive information across publicly accessible networks such as the Internet, businesses seek assurance that the data received actually came from the true source of the data, and not from an interloper, and that the data transmitted was not altered during transmission. For TCP/IP networks, it is necessary that this assurance extend not just to the user data within the packet, but to the addressing information in the packet as well. SafeNet provides this assurance by applying data authentication techniques to every secured packet. These techniques are defined in two security standards: IETF RFC 1827 (Encapsulated Security Payload, or ESP Header) and ANSI X9.9 Message Authentication.

At the time of transmission, an IRE security device encrypts user data to ensure privacy. An additional security header, the ESP header, is added to the packet. The entire contents of the packet (including the address) is then submitted to SHA-1 secure hashing, to generate a Message Authentication Code, or MAC. The MAC is installed in the ESP header. An encrypted counter message is then appended. Figure 2 depicts this process.

After transmission, the receiving IRE device removes the ESP header and decrypts the packet. The device then re-generates the MAC. If the MAC sent with the packet matches the MAC generated at the receiving device, then the data has been transmitted without alteration. Use of the encrypted counter separately tracks the receipt of secured packets in sequence, and assures that any illegitimate copies of data already received (as in an intrusion process commonly employed by hackers, called a replay attack) are instantly exposed and discarded.

SafeNet™

Figure 2
Conversion of an Unsecured Packet into an Encrypted, Authenticated Packet



Address Filtering

Address filtering allows SafeNet products to be configured to support an 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 the system.

Tunnel Processing

Tunnel processing or "Address Hiding" may be required for a SafeNet encryptor that is in a private network or behind a firewall to communicate across the public Internet. 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 so that the private IP addresses are received by the proper party.

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. Key Management in the 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 device serial 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 are only safely encrypted under another key.
- The key exchange process operates according to ANSI Standard X9.17.

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

Key Types

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 – KMO
A manually-entered or randomly-generated DES key used to encrypt Master Keys stored electronically in the SafeNet/Security Center. KMO 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. KMO is stored in a cryptographic module 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 KMO.

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.

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 KMO 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 or end user responsible for configuring the SafeNet encryptor. At the remote encryptor, the Security Officer or end user inserts the smartcard into the encryptor and runs a configuration utility that 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.

The 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 Key. The Session Key is then used by each device to encrypt/decrypt and authenticate all data being exchanged in the secure communications session.

SafeNet™

Key Storage:

The Storage Key (KMO) is only resident in the S/SC. The key is stored in a separate tamper-proof cryptographic module that is installed in the S/SC workstation. Once entered, the value of KMO 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 KMO 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 can neither 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 until the key expires, at which time the Session Key is erased.

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 KMO 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 the User Authentication section, the random number challenge and user PIN combination is encrypted under the User Key as part of the ANSI X9.26 user authentication process.

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. SafeNet products have been developed with specific roles and services defined to allow easy incorporation into a company-specific security policy.

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, user and device enrollment, 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 given to setting up user access to the S/SC. It is important that the individuals provided access to this system are trustworthy because 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 who has access to all areas of the workstation, to maintenance personnel who have limited access to only the backup and archive features. The six distinct levels of access to the S/SC are summarized below.

SafeNet™

Security Administrator
This is the highest level of access available to users of the system. The Security Administrator is capable of establishing access levels for security personnel, modifying critical configuration settings, authorizing network devices, administering access controls, setting up event log backups, reviewing and clearing alert messages, and accessing diagnostic messages.

System Administrator
The System Administrator has essentially the same capabilities as the Security Administrator, with the exception that he/she cannot revise 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 capable only of viewing the Event Log.

Maintenance
This level is used in situations where employees, other than security personnel and administrators, would be backing up S/SC computer databases, and archiving and backing up the Event Log.

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. Services related to operation of the encryptor include encryptor configuration, self-test, and status indication. While the encryptors provide all these services, the primary purpose of the devices is the transfer of secure data. As such, the Comprehensive Security Services Section of this document describes in detail the elements that make up a secure data service: data encryption, user authentication, packet authentication, address and socket filtering, and tunnel processing.

The encryption devices may support four different roles: configuration, user with authentication, user authentication without authentication, and remote manager. The remote encryptors support all four roles. The S/LAN VPN Encryptor supports the configuration and remote manager roles. A summary of the different roles follows.

Configuration
The security officer or the end user can be responsible for configuring the

encryptor. Configuration can be done using a smartcard (or diskette for SafeNet/Soft) 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. In the case of SafeNet/Soft, only an alphanumeric PIN is required.

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 S/SC. The S/SC provides configuration downloads and key management. The S/SC is capable of preventing the devices from performing secure communications.

As an example of secure communications using SafeNet products, the steps below outline the process of a remote user gaining access to a secure website protected by a SafeNet/LAN VPN Encryptor that requires user authentication before allowing access.

1. The user clicks on a SafeNet Load UA PIN icon or menu listing and enters his/her PIN.
2. The user starts an Internet browser and calls his/her Internet Service Provider.
3. Through a bookmark or known URL the user attempts to access a secure web site.
4. Although network delays can influence the total time for session establishment, the following process generally occurs in less than two seconds, invisibly to the user:

    - The remote encryptor recognizes that the IP address requires encryption and sends a "Request for Service Initiation" (RSI) to the S/LAN VPN Encryptor.
    - The S/LAN forwards the request to the S/SC, noting that user authentication is required.
    - The S/SC sends a random number challenge to the remote encryptor
    - The remote encryptor answers the challenge by returning a one-time password based on the random number challenge and the user PIN, encrypted under the User Key.
    - The S/SC verifies the authentication response and sends two copies of a random one-time session key to the S/LAN VPN Encryptor, one encrypted under the S/LAN's master key and one encrypted under the remote encryptor's master key.
    - The S/LAN decrypts it's copy of the session key and sends on the remote encryptor's copy.
    - The remote encryptor decrypts its copy of the session key.
    - An encrypted tunnel has been formed between the remote encryptor and the S/LAN VPN Encryptor. All data communications are now automatically encrypted and authenticated.

5. When a secure session is established, a S/DIAL or S/DIAL-R user will see a green light turn on, indicating session key delivery. A S/Soft or S/Smart user will see the background of the SafeNet icon turn green.
6. The secure web page is downloaded to the user. While waiting for session establishment, the user sees what appears to be normal browser activity. A message such as "Host contacted, waiting for reply" appears in the status area of the browser.

Appendix A provides the explicit detail of secure session establishment

SafeNet™

Appendix A: SafeNet Secure Session Establishment

This appendix explains the steps required to establish a secure session over the Internet between a remote client and a target host computer. The network diagram shown in figure A-1 depicts the placement and IP addresses of the client, the target host, the management center, and the encryption devices. Definitions are as follows:

SNR: Serial number of the remote encryptor.

R.R.R.R: Address of the remote encryptor that initiates the secure session

C.C.C.C: Address of the remote client that is protected by R.R.R.R. In a remote dial-up application, R.R.R.R = C.C.C.C and is usually assigned dynamically by the remote client's ISP.

SNP: Serial number of the peer encryptor.

P.P.P.P: Address of the peer encryptor that protects the target host computer.

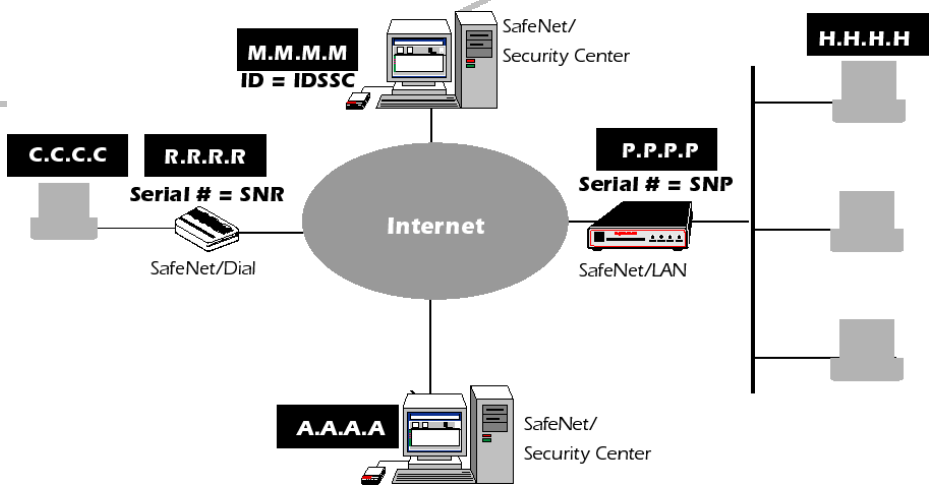
H.H.H.H: Address of the target host computer that is protected by P.P.P.P.

IDSSC: The ID of the SafeNet/Security Center (S/SC).

M.M.M.M: Address of the management center, the SafeNet/Security Center. The SafeNet/Security Center initiates and monitors the client authentication process, records security events, and provides one-time session keys to the encryption devices.

A.A.A.A: Address of an alternate management center. If there is no alternate management center defined, M.M.M.M = A.A.A.A.

Figure A-1:
Secure Session Establishment Network



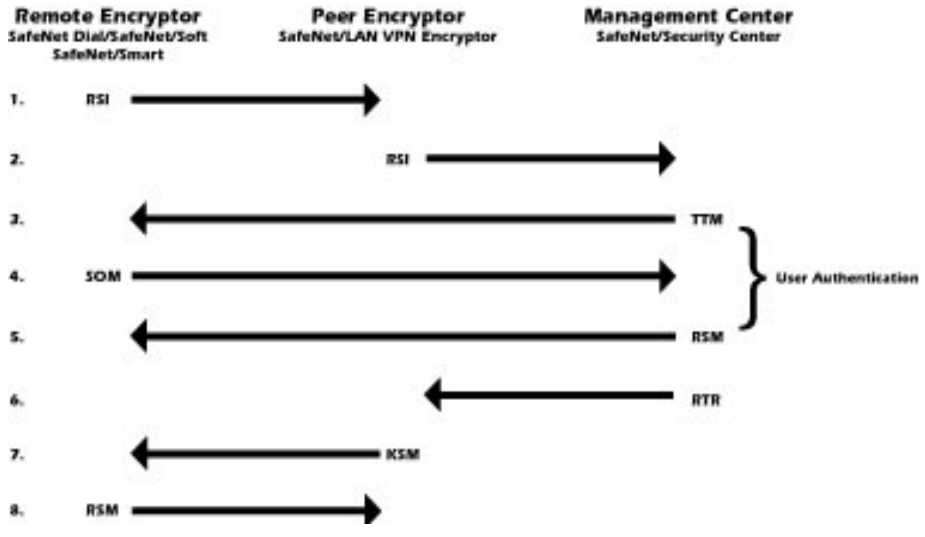
SafeNet encryptors monitor all IP traffic to and from the protected client or host. IP addresses of incoming and outgoing messages are compared to a set of rules kept in the encryptor's filter table. If an IP address matches a rule requiring encryption, then the process of establishing a secure session begins.

For instance, suppose a user types in www.ire.com into their web browser and ire.com is a site requiring encryption. The client PC will first go out to the DNS to resolve the URL. When the IP address is sent back, the client PC will attempt to begin to send IP packets to that address. The encryptor will match the IP address against a filter rule and attempt to establish a secure session before communications will be allowed to proceed.

In order to establish a secure session, Cryptographic Service Messages or CSM's are sent between the encryptors and between the encryptors and the S/SC

management center. Secure session establishment with user authentication requires six distinct CSM's and a total of eight steps. Figure A-2 shows the flow of CSMs required to establish a secure session. The steps and CSM's are defined as follows:

1. RSI: Request for Service Initiation: A request for a session key sent from the remote encryptor to the peer encryptor.
2. RSI: Request for Service Initiation: A request for a session key sent from the peer encryptor to the S/SC management center. It is the configuration of the peer encryptor that determines if user authentication is required before issuance of session keys. The peer encryptor may require (always authenticate), prefer (authenticate if possible), or not require (never authenticate) user authentication.
3. TTM: Time-varying Transfer Message: A user authentication challenge message sent from the S/SC to a remote encryptor. Before issuing session keys, the S/SC checks the configuration of the peer encryptor and the remote encryptor. If the peer encryptor requires or prefers authentication, and the remote encryptor is configured to support user authentication, then the S/SC sends a TTM to the remote encryptor to begin the user authentication process.
4. SOM: Sign On Message: A response to the user authentication challenge sent from the remote encryptor to the S/SC
5. RSM: Response to Service Message: An acknowledgment sent back to the remote encryptor by the S/SC to indicate receipt and acceptance of the SOM. This completes the user authentication process.
6. RTR: Response To Request: A message sent by the S/SC in response to an RSI from a peer encryptor. The RTR contains two sets of encrypted one-time session keys, one for the peer encryptor and one for the remote encryptor. The peer encryptor picks off its copy of the session key from the RTR and relays the remote encryptor's copy via the KSM in step 7.
7. KSM: Key Service Message: A message sent by the peer encryptor in response to an RSI from the remote encryptor (step 1). The KSM contains the encrypted one-time session key.
8. RSM: Response to Service Message: An acknowledgment sent back to the peer encryptor by the remote encryptor to indicate successful receipt of the KSM. This completes secure session establishment. The remote encryptor and peer encryptor each decrypt the one-time session key and use it to encrypt all subsequent communications between them. An encrypted tunnel has been established.



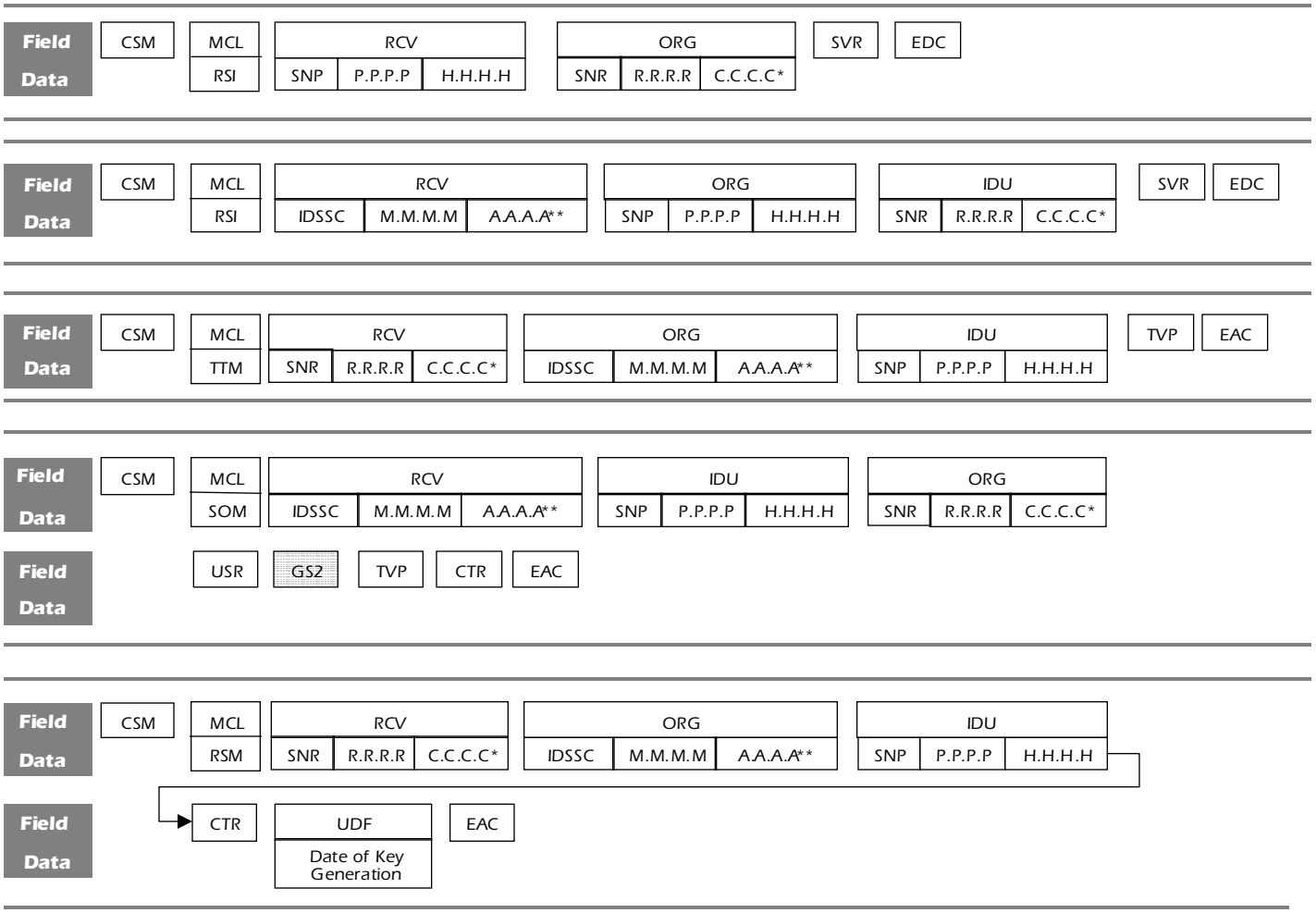
SafeNet™

Establishment of a secure session using SafeNet products and the contents of the CSM's are governed by ANSI X9.17, the standard for secret key management, and ANSI X9.26, the standard for user authentication. In general, the contents of the CSM's are sent in the clear, i.e. non-encrypted. The encrypted portions of the CSM's are:

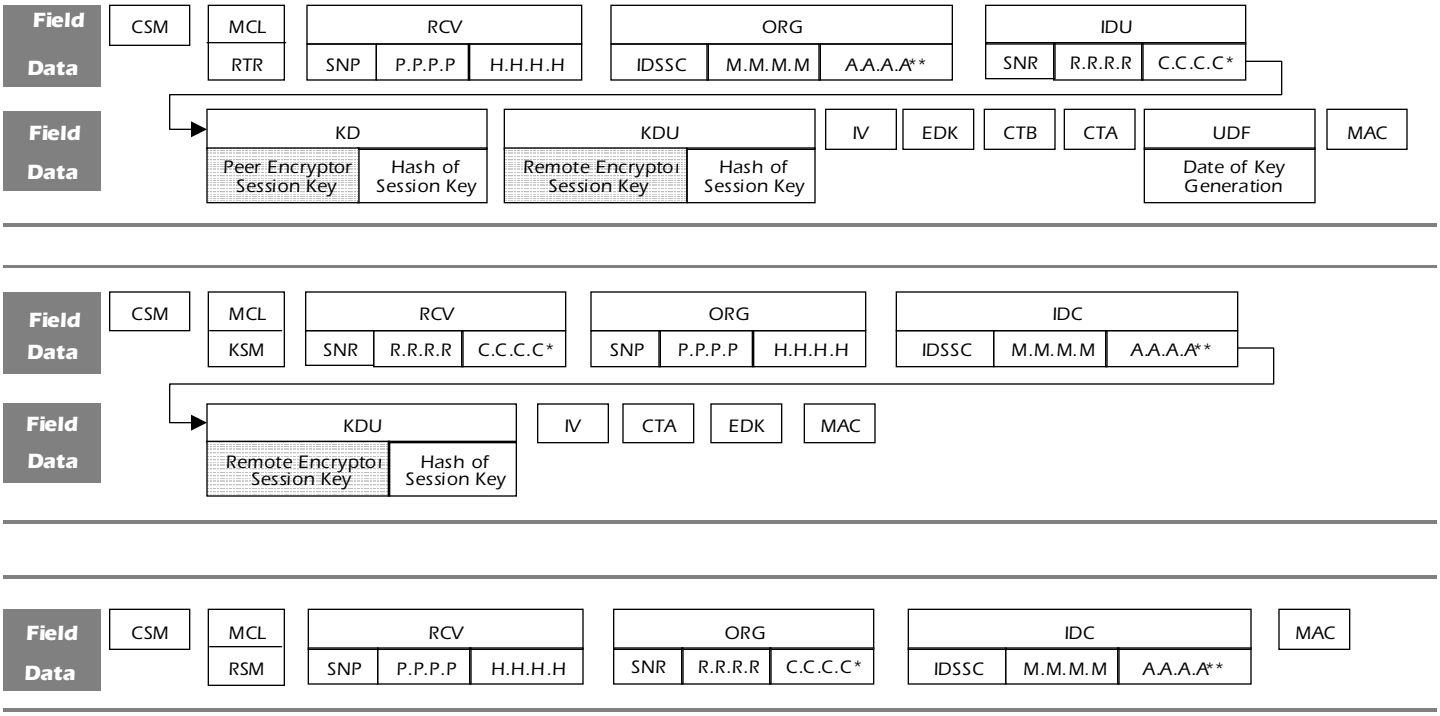
- The response to the TTM challenge sent in the SOM by the remote encryptor to the S/SC management center
- The session keys sent in the RTR by the S/SC to the peer encryptor
- The session key sent in the KSM by the peer encryptor to the remote encryptor

Figure A-3 shows the message format for each of the eight CSM's required for secure session establishment with user authentication. Encrypted fields are shaded.

Figure A-3: CSM Message Formats



(FIGURE A-3: CSM MESSAGE FORMATS)



* In a remote dial-up application R.R.R.R = C.C.C.C

** If there is no alternate S/ SC M.M.M.M = A.A.A.A

Lined fields are encrypted

CSM Fields and Values

The CSM fields and possible values for each field are defined below. Encrypted fields are underlined.

- **CSM** - Cryptographic Service Message - group of messages for the exchange of keys and notifications
- **CTA** - Counter for party A - the counter associated with the master key for the remote encryptor
- **CTB** - Counter for party B - the counter associated with the master key for the peer encryptor
- **CTR** - Counter - counter associated with the number of times the user has changed their User PIN
- **EAC** - Encrypting Authentication Code - a checksum of a user authentication CSM used to ensure accuracy
- **EDC** - Error Detection Check - a checksum of the CSM used to ensure accuracy
- **EDK** - Effective Date of Key - Date the key expires
- **GS2** - The encrypted challenge response to the TTM. It is calculated by XOR'ing a user entered PIN and the TVP sent in the TTM, and then encrypting the result with the User Key.
- **IDC** - Identification of the key management Center - the key management center involved in this key establishment composed of the key management

center's ID, IDSSC, the key management center's IP address, M.M.M.M, and either the same address or the address of an alternate key management center, A.A.A.A.

- **IDU** - Identification of the Ultimate recipient - the encryptor involved in this key establishment other than the ORG or RCV
    - If the ultimate recipient is the remote encryptor then the IDU is composed of the remote encryptor's serial number, SNR, the remote encryptor's IP address, R.R.R.R, and the remote client's IP address, C.C.C.C. In a remote dial-up application, R.R.R.R = C.C.C.C.
    - If the ultimate recipient is the peer encryptor then the IDU is composed of the peer encryptor's serial number, SNP, the peer encryptor's IP address, P.P.P.P, and the target secured IP address, H.H.H.H.
    - If the ultimate recipient is the Key Management Center then the IDU is composed of the key management center's ID, IDSSC, the key management center's IP address, M.M.M.M, and either the same address or the address of an alternate key management center, A.A.A.A.
- **IV** - Initialization Vector - a number used by the DES engine to determine where to start when encrypting or decrypting with the session key
- **KD** - Key encrypting Data - the fields for delivery of the one-time session key to the peer encryptor: The session key encrypted with the peer encryptor's master key, and a hash of the session key with the encrypted session key.
- **KDU** - Key encrypting Data for the Ultimate recipient - the fields for delivery of the one-time session key to the remote encryptor: The session key encrypted with the remote encryptor's master key, and a hash of the session key with the encrypted session key.
- **MAC** - Message Authentication Code - a code used to authenticate the CSM based upon the use of a key
- **MCL** - Message Class - the type of CSM message sent
    - **RSI** - Request for Service Initialization - a request for a session key
    - **TTM** - Time-varying Transfer Message - a user authentication challenge message containing the Time Varying Parameter TVP field
    - **SOM** - Sign On Message - a user authentication response message containing the GS2 field.
    - **RSM** - Response to Service Message - an acknowledgment sent back to an encryptor by the S/SC or another encryptor to indicate successful receipt and acceptance of a previous CSM.
    - **RTR** - Response To Request - the message sent by the SafeNet/Security Center in response to an RSI from a peer encryptor
    - **KSM** - Key Service Message - the message sent by the peer encryptor in response to an RSI from the remote encryptor.

- **ORG** - Originator - the originator of the CSM message
    - If the originator is the remote encryptor then the ORG is composed of the remote encryptor's serial number, SNR, the remote encryptor's IP address, R.R.R.R, and the remote client's IP address, C.C.C.C. In a remote dial-up application, R.R.R.R = C.C.C.C.
    - If the originator is the peer encryptor then the ORG is composed of the peer encryptor's serial number, SNP, the peer encryptor's IP address, P.P.P.P, and the target secured IP address, H.H.H.H.
    - If the originator is the Key Management Center, then the ORG is composed of the key management center's ID, IDSSC, the key management center's IP address, M.M.M.M, and either the same address or the address of an alternate key management center, A.A.A.A.
- **RCV** - Receiver - the intended receiver of the CSM message
    - If the intended receiver is the remote encryptor then the RCV is composed of the remote encryptor's serial number, SNR, the remote encryptor's IP address, R.R.R.R, and the remote client's IP address, C.C.C.C. In a remote dial-up application, R.R.R.R = C.C.C.C.
    - If the intended receiver is the peer encryptor then the RCV is composed of the peer encryptor's serial number, SNP, the peer encryptor's IP address, P.P.P.P, and the target secured IP address, H.H.H.H.
    - If the intended receiver is the Key Management Center, then the RCV is composed of the key management center's ID, IDSSC, the key management center's IP address, M.M.M.M, and either the same address or the address of an alternate key management center, A.A.A.A.
- **SVR** - Service Request - used to notify the key management station of the options of the requesting device
- **TVP** - Time Varying Parameter - a random number challenge sent to a client device used for user authentication
- **UDF** - User Definable Field - contains various fields for key applicability. Possible values are:
    - D - Date the key expires
    - F - Filter mask for the key
    - T - Tunneling enabled or disabled
    - V - Virtual Remote Subnet negotiation
- **USR** - User - the ID of the party using the remote encryptor. USR allows the key management center to identify the User Key and User PIN involved in the calculation of GS2.