

---

*Financial  
Services  
Security*



*Network Security  
Products Profile*

**Technical Contact Information**

If further information regarding technical content is required, please contact:

BITS Financial Services Security Lab

bits@fsround.org

Tel. 202.289.4322

Fax: 202.289.3562

---

<b>Originating Author:</b>	Randy Gale, Regional Director - Information Security Practice, Predictive Systems, Inc.
<b>Profile Leader/Workgroup Chair:</b>	<b>Terry Leahy</b> , VP, Corporate Information Security Services, Wells Fargo & Company

---

*BITS Security Lab Network Security Profile Workgroup members (primary contributors/organizations are in **bold**):*

<b>Representative</b>	<b>Organization</b>	<b>Representative</b>	<b>Organization</b>
Brian Cregg	Allfirst Financial, Inc.	Jim St. Clair	U.S. Department of the Navy
Brian Ekkebus	Northern Trust Corporation	John C. Walp	M&T Bank Corporation
Colin Meagher	J.P. Morgan Chase & Co.	<b>John Walsh</b>	<b>Allfirst Financial, Inc.</b>
Craig Shorter	First Tennessee National Corporation	Mary Jane Bolling	Capital One Financial Corporation
Dennis Smith	Mellon Financial Corporation	Robert Bednar	Mellon Financial Corporation
<b>Eric Guerrino</b>	<b>The Bank of New York Company, Inc.</b>	Robert Burch	The PNC Financial Services Group, Inc.
Gary Conner	BB&T Corporation	<b>Ron Dinehart</b>	<b>IBJ Whitehall Financial Group</b>
Gene Fredriksen	Raymond James Financial, Inc.	Ron Howard	Whitney Holding Corporation
<b>Gordon Martin</b>	<b>Wells Fargo &amp; Company</b>	Sean Amon	Nationwide
Gregory Blair	Fortis, Inc./Assurant Group	Steve Wyllie	FleetBoston Financial Corporation
<b>Jim Brown</b>	<b>Marshall &amp; Ilsley Corporation/Metavante</b>	<b>Terry Griffith</b>	<b>Capital One Financial Corporation</b>

### Profile Feedback

If you have any comments (technical or otherwise) regarding this profile, please send an email to bits@fsround.org. Include the profile name along with your name, email address, telephone and fax number, and indicate whether you would like to be contacted. *Please note: The BITS Security Lab will take all comments under advisement, but reserves the right to include or exclude comments received in the final criteria.*

---

### Network Security Products Profile – Version Control History

Note: **Bold** in Version column indicates a Public Release.

Version / Date	Changes
0.90 – 0.91 (May 2000)	DRAFT – Creation of initial draft (Predictive Systems/Profile Leader/BITS)
1.00 – 1.14 (May 2000 – May 2001)	DRAFT – FI Workgroup review (FI Distribution Only)
1.15 – June, 2001	DRAFT – Post May 10 and 11 Workshop with FIs and TPs
1.17 – Aug 2001	DRAFT – Prior to public comment posting
<b>1.18 – Nov 2001</b>	FINAL – To public comment and ready for testing

# Table of Contents

---

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>2. CRITERIA FOR THE ADMINISTRATION AND OPERATION OF NETWORK SECURITY PRODUCTS.....</b>	<b>6</b>
<b>2.0 SECURITY FEATURES.....</b>	<b>6</b>
2.1 IDENTIFICATION.....	7
2.2 AUTHENTICATION.....	7
2.3 AUTHORIZATION.....	10
2.4 CONFIDENTIALITY.....	11
2.5 DATA INTEGRITY.....	12
2.6 AUDIT.....	13
2.7 DATA DISPOSAL.....	14
2.8 SYSTEM INTEGRITY.....	15
2.9 SECURITY ADMINISTRATION.....	16
2.10 GUIDANCE.....	17
2.11 NON-REPUDIATION (DESIRED).....	18
3.0 PRODUCT FUNCTIONALITY.....	19
4.0 SCALABILITY.....	20
<b>3. REQUIRED FUNCTIONAL CRITERIA FOR NETWORK SECURITY PRODUCTS.....</b>	<b>21</b>
3.1 INTRODUCTION.....	21
3.2 ACCESS MEDIATION.....	21
3.3 USER MANAGEMENT.....	23
3.4 STORAGE OF SECURITY DATA.....	24
3.5 SYSTEMS MANAGEMENT AND CONFIGURATION.....	24
<b>4. DESIRED FUNCTIONAL CRITERIA FOR NETWORK SECURITY PRODUCTS.....</b>	<b>26</b>
4.1 INTRODUCTION.....	26
4.2 PRODUCT CONFIGURATION.....	26
<b>5. FUNCTIONAL CRITERIA NETWORK SECURITY SYSTEMS PRODUCT SUB-CLASSES.....</b>	<b>28</b>
5.1 INTRODUCTION.....	28
5.2 FUNCTIONAL CRITERIA FOR FIREWALL PRODUCTS.....	29
5.3 FUNCTIONAL CRITERIA FOR VIRTUAL PRIVATE NETWORK (VPN) PRODUCTS.....	31
5.4 FUNCTIONAL CRITERIA FOR LINK LAYER ENCRYPTION PRODUCTS.....	33
<b>APPENDIX A: INDUSTRY STANDARDS.....</b>	<b>35</b>
<b>APPENDIX B: BIBLIOGRAPHY.....</b>	<b>36</b>
<b>APPENDIX C: GLOSSARY OF TERMS.....</b>	<b>37</b>

# 1. Introduction

---

## Overview

Corporate computing environments have evolved from environments where data and resources were concentrated in self-contained data centers to extensively distributed computing architectures. Today's information and resources are routinely distributed over trusted and untrusted networks. Connection to the Internet, an untrusted network, can expose trusted and closed corporate networks to a wide range of security threats. Employing network security products mitigates many of the risks associated with connectivity to untrusted networks.

There are a variety of network security technologies, and focal points for these technologies, in private networks with connections to public networks like the Internet. A single set of criteria will not apply to all of the technologies. In other words, a criterion that is essential to one technology may be meaningless to another.

Consequently, this profile is organized into several parts. The first lists administration and operational criteria that are common to all security technologies. The second part lists criteria that are specific to typical network security system products. The third lists any optional criteria for network security system products and the fourth lists criteria applicable to distinct sub-classes of network security system products. Network security product's help to provide security by allowing trusted separation between networks, controlling communication between nodes and/or encrypting such communication.

Examples of the network security system sub-classes that this product profile would apply to are:

### *Firewalls*

Products in this sub-section enable the establishment of allowable transmissions between hosts across untrusted networks, including the Internet.

### *Virtual Private Networks*

These products provide functionality that allows controlled interconnection of private networks across a public network.

### *Link Layer Encryption*

Products in this sub-section provide network encryption services suitable for protecting the confidentiality of information.

These sub-classes will encompass software and hardware products that help control authorized and unauthorized access to private networks, as well as confidentiality of transmissions.

There are many important security focal points within and between networks, such as:

- Remote Access
- OS-based Network Security
- SSL-based Security
- IPSec-based Security
- Secure Routers

However, the following focal points are more properly addressed by other product profiles and are outside the scope of the Network Security profile:

- Authentication
- Access Control and Administration
- Monitoring and Intrusion Detection
- Application Security
- Operating System Security

Network Security is important to the interoperability of the Internet and private networks as a basis for authorized network access control and transmission confidentiality. In general, the “strength” of the network security system should be proportional to the value of the assets or data being protected. It is understood that it is usually not possible to know the value of an asset at the time of testing for a network security system product. Therefore, this document assumes that the protected asset is of the highest value and lists an extensive set of applicable criteria.

The criteria have been derived and expanded from the Master Security Criteria (MSC<sup>1</sup>). Specifically, Section 2 of this document is a complete mapping of the MSC related to the Operations and Administration of products in this profile’s product class. It is recommended that readers of this document review the MSC and use it as a reference document to this profile.

---

<sup>1</sup> Refer to Appendix B of this document for MSC version used.

## Mandatory and Desired Criteria

Each criterion will be identified as being *required* or *desired*<sup>2</sup>. A product will earn the *BITS Tested Mark* only if it meets all the *mandatory* criteria within Section 2, “Criteria for the Administration and Operation of Network Security Products,” Section 3, “Required Functional Criteria for Network Security Products,” and the appropriate subclass of Section 5, “Functional Criteria for Network Security Systems Product Sub-classes.” In other words, a product will not merit a *BITS Tested Mark* if it misses any one mandatory criterion.

In this document, *mandatory* criteria will use the verb “shall,” while *desired* criteria will use the verb “should.”

Additionally, some criteria are identified within the profile document as *desired*. These criteria are not required to obtain the *BITS Tested Mark*, but compliance with these criteria will be noted in the final Test Report. *Desired criteria are recognized by the financial services industry as advantageous and may become requirements in the future.*

## Boundaries and Underlying Platforms

A number of criteria outlined in this document may be addressed through security features of underlying platforms, rather than through the product itself. Rather than requiring all security functionality to be provided by the standalone systems, the criteria and process allow the product to rely on an underlying platform (e.g., an operating system) for security. To support this, the process allows the Technology Provider and the Testing Lab to define the “boundaries” of the test environment, which delineate the system to be tested. It is anticipated that this boundary will include the product itself and the underlying hardware and software. It is important to note, however, that the criteria will be applied equally to all components within that boundary.

Example: A firewall relies on the underlying operating system to provide scalable operation. This may be sufficient to meet the criteria for scalability. If, however, during the testing, a vulnerability is found in the operating system software that renders the system non-compliant with any of the Profile criteria, the firewall product will not earn the *BITS Tested Mark* unless the vulnerability is addressed. Whether or not the vulnerability lies in another vendor’s product will

---

<sup>2</sup> A criterion shall be considered *required* unless it is explicitly identified as being *desired*.

be considered irrelevant, since it has been defined as part of the test environment within the boundary.

## Test Plans and Profiles

It is important to note that actual testing of individual products will be conducted against a test plan produced from this profile. Each product undergoing testing will have a specific test plan developed. *It is entirely possible that certain criteria will be implemented differently, and thus tested differently, in two similar products.*

Network security products will be tested within a standard configuration and environment. Systems that consist of only a single system will be tested with the hardware and software supplied by the manufacturer. Systems that include a dedicated management console will be tested with the management console controlling the subordinate system(s). The management console and subordinate systems will each consist of a supporting platform and user interfaces.

## Common Terms Used in This Profile

In this section, we list definitions of terms that are important or frequently used in the remainder of this profile. Please refer to “Appendix C: Glossary of Terms” for a complete list of terms used.

TERM	DEFINITION
<b>access control</b>	<i>A mechanism for limiting use of some resource to authorized users. [1]</i>
<b>audit</b>	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
<b>authentication</b>	<i>The process of reliably determining the identity of a communicating party. [1]</i>
<b>authenticator</b>	<i>The method, material or credential used to create and/or implement authentication bindings, such as a password, PIN number, token seed or smart card seed.</i>
<b>confidentiality</b>	<i>The property of not being divulged to unauthorized parties. [1]</i>
<b>integrity</b>	<i>The quality of being uncorrupted. Message integrity refers to the state of a message not being modified while in transit. File integrity refers to the state of files not being modified while in storage. [2]</i>
<b>log file</b>	<i>A file that lists actions that have occurred. [2]</i>
<b>Master Security Criteria (MSC)</b>	<i>This document contains the BITS Security Lab criteria that will be used to generate product-specific criteria. The criteria in this document will be used to develop the individual Product Security Profiles. MSC version 3.0 will be referenced for this profile.</i>
<b>non-repudiation</b>	<i>The property of a scheme in which there is proof of who sent a message that a recipient can show to a third party, and the third party can independently verify the source. [1]</i>
<b>privileged user</b>	<i>A user of a computer or system who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions. [1]</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>product administrator</b>	<i>In the scope of this profile, this role is associated with a user having higher privilege at the product's configuration level. This user (role) may be the same as that of the system administrator, but could also be different.</i>
<b>system</b>	<i>Within the scope of this profile, "system" is used to imply the totality of the product and the mediation device (if any) that needs to be tested.</i>
<b>system administrator</b>	<i>In the scope of this profile, an individual (user) who has higher privilege at the operating system level.</i>
<b>user-ID</b>	<i>A number or name that is unique to a particular user of a computer or group of computers that share user information. The operating system uses the user-ID to represent the user in its data structures, e.g., the owner of a file or process or the person attempting to access a system resource.</i>

## 2. Criteria for the Administration and Operation of Network Security Products

---

### Security Features

For each of the subclasses listed below, this section lists the minimal functionality in terms of security features expected in products of that subclass. This section lists the security criteria from the Master Security Criteria document that are common to all products and specifically apply to the administration and operation of most network encryption, VPN and firewall products. The criteria are grouped according to the functionality provided by a typical Network Security product, resulting in the following criteria groups listed below. Examples of the functionality are also listed for each group. The criteria are categorized according to the following major sections in the Master Security Criteria (MSC):

1. Identification
2. Authentication
3. Authorization
4. Confidentiality
5. Data Integrity
6. Audit
7. Data Disposal
8. System Integrity
9. Security Administration
10. Guidance
11. Non-Repudiation (Desired)

It may be that the composition of a particular firewall, VPN or link layer encryption product does not operate on an application (OSI model) or end-user level. However, users who are administrators, or are providing support and maintenance for the network security products, are operators of the product and are considered users of the system. Therefore, they are governed by these criteria.

## 2.1 Identification

Identification is the process of recognizing a user's unambiguous and auditable identity with the help of an identifier that is typically referred to as the user-ID. In general, the user-ID need not be confidential. It is the unambiguous name of a user through which the user can be held accountable. All actions initiated by a user need to be associated with the corresponding user-ID. The security-related requirements in relation to user identification are provided in this section.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.1 Identification<sup>3</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.1.1	Required	
2.1.2	Required	
2.1.3	Required	
2.1.4	Required	
2.1.5	Required	
2.1.6	Required	<i>In addition, these attributes should and shall be associated with the account. Furthermore, any security-related attributes that are maintained should and shall be stored securely so that their confidentiality and integrity are protected.</i>

## 2.2 Authentication

Authentication is the process of verifying the claimed identity of a user. Depending on the system and the application, different kinds of authenticators can include passwords, tokens, smart cards, key-based authenticators, voice recognition and/or a retina scan. Regardless of

---

<sup>3</sup> "Identification" is identified as: The system shall have the capability of associating a user with an unambiguous identifier (e.g., user-ID) by which the said user shall be held accountable for the actions and events initiated by that user.

what type is used, it is critically important to minimize the compromise of an authenticator. Mechanism requirements have been divided into three categories: **General** applies to all types of authentication mechanisms; **Knowledge-** and **Possession-based** addresses mechanisms such as passwords; and **Personal Characteristics-based** provides guidelines for biometric mechanisms. Following are the security-related requirements for each type.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.2: Authentication<sup>4</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
<b>Subsection 2.2.1: General Mechanism Requirements</b>		
2.2.1.1	Required	
2.2.1.2	Required	
2.2.1.3	Required	
2.2.1.4	Required	
2.2.1.5	Required	
2.2.1.6	Required	
2.2.1.7	Required	
2.2.1.8	Required	
<b>Subsection 2.2.2: Knowledge- and Possession-based Mechanism Requirements</b>		
In the process of authentication, security information has to be exchanged to verify the user's identity. This feature is focused on specific requirements for mechanisms that support security information known and possessed by the user and submitted for validation.		
2.2.2.1	Required	
2.2.2.2	Required	
2.2.2.3	Required	
2.2.2.4	Required	

<sup>4</sup> "Authentication" is defined as: The system shall offer features to verify the claimed identity of a user before allowing system access to the said user.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<p><b>MSC Section 2.2: Authentication<sup>4</sup></b></p> <p>Note: Criteria in this section are applicable to the <u>administration and operation of the product</u>, unless specifically identified in the “Comment or Rationale” column.</p>		
2.2.2.5	Required	
2.2.2.6	Required	
2.2.2.7	Required	
2.2.2.8	Required	
2.2.2.9	Required	
2.2.2.10	Required	
2.2.2.11	Required	
2.2.2.12	Required	
<p><b>Subsection 2.2.3: Personal Characteristics-based Mechanism Requirements (DESIRED)</b></p> <p>This type of authentication mechanism securely captures the physical characteristics (e.g., fingerprint) of the user and provides that data to the authentication process for validating the identity of the user.</p> <p><b>NOTE:</b> The classification of “DESIRED” for this entire subsection indicates that the product submitted for evaluation may not need to comply with the criteria in this section. For the product to be recognized as providing “personal characteristics-based authentication mechanisms,” it is <u>not</u> a DESIRED section; thus, if the product is claiming it provides these functions, it must fully comply with all criteria in this subsection (2.2.3).</p>		
2.2.3.1	Required	<i>See note above.</i>
2.2.3.2	Required	<i>See note above.</i>
2.2.3.3	Required	<i>See note above.</i>

## 2.3 Authorization

The authorization feature is focused on the controls associated with establishment of a session with the system, invocation of operations- or services-oriented tasks, or the access of information while it is stored.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.3: Authorization<sup>5</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.3.1	Required	
2.3.2	Required	
2.3.3	Required	
2.3.4	Required	
2.3.5	Required	<i>Requiring an administrator to reinstate the locked account provides the industry with the correct level of control over the threatened account.</i>
2.3.6	Required	
2.3.7	Required	
2.3.8	Required	
2.3.9	Required	
2.3.10	Required	
2.3.11	Required	
2.3.12	Required	
2.3.13	Required	<i>This criterion points out that the system must ensure that all resources are protected from access by default. Starting from this position, the system ensures that no resource access can take place without an active decision by the administrator to establish the permission.</i>
2.3.14	Required	

<sup>5</sup> "Authorization" is defined as: The system shall offer features to support the following restrictions: no user shall be allowed access to the system without Identification and Authentication; and no user shall be allowed access to a resource (e.g., transaction, data, process, etc.) of the system unless specifically authorized to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.3: Authorization<sup>5</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.3.15	Required	<i>This criterion refers to ports; however, it is applicable to network interfaces, which are a part of, or secured by, network security products as well.</i>
2.3.16	Required	
2.3.17	Required	
2.3.18	Required	
2.3.19	Required	
2.3.20	Required	<i>This feature is essential to ensure that intended authorization assignments cannot be bypassed by any user or administrator. When the system provides a bypass feature, then authorization controls are not consistent and activities performed through the bypass may go unrecorded by audit measures.</i>

## 2.4 Confidentiality

The confidentiality protection feature is focused on protecting sensitive information from unauthorized disclosure while the information is being generated, stored, manipulated or forwarded. The security-related requirements in relation to confidentiality include the following:

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.4: Confidentiality<sup>6</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.4.1	Required	
2.4.2	Required	

<sup>6</sup> “Confidentiality” is defined as: The system shall offer features to ensure that sensitive information shall be communicated and stored in a way such that only authorized users are allowed access.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.4: Confidentiality<sup>6</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.4.3	Required	
2.4.4	Required	
2.4.5	Required	
2.4.6	Required	
2.4.7	Required	
2.4.8	Required	
2.4.9	Required	
2.4.10	Required	
2.4.11	Required	
2.4.12	Required	
2.4.13	Required	
2.4.14	Required	
2.4.14	Required	

## 2.5 Data Integrity

This feature is focused on preventing and detecting unauthorized modification of data that is associated with a user, the system itself, or the communications path. The security-related requirements in relation to data integrity include the following:

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.5: Data Integrity<sup>7</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.5.1	Required	
2.5.2	Required	
2.5.3	Required	
2.5.4	Required	
2.5.5	Required	
2.5.6	Required	
2.5.7	Required	
2.5.8	Required	
2.5.9	Required	
2.5.10	Required	

## 2.6 Audit

This feature has to provide adequate capabilities to investigate unauthorized activities after an event, so that the proper remedial action can be taken. This implies the recording of security-relevant events into an audit log that can be analyzed by the administrator. The security-related requirements in relation to audit include the following:

---

<sup>7</sup> "Data integrity" is defined as: The system shall offer features to ensure that either: the data shall not be modified or altered without authorization in either storage or in transit; or any unauthorized modification of data shall yield an auditable security-related event.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.6: Audit<sup>8</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.6.1	Required	
2.6.2	Required	
2.6.3	Required	
2.6.4	Required	
2.6.5	Required	
2.6.6	Required	
2.6.7	Required	
2.6.8	Required	
2.6.9	Required	
2.6.10	Required	
2.6.11	Required	
2.6.12	Required	

## 2.7 Data Disposal

This feature is focused on protecting sensitive information from unauthorized recovery and subsequent disclosure from internal system memory and storage after authorized use. The security-related requirements in relation to data disposal include the following:

---

<sup>8</sup> "Audit" is defined as: The system shall offer features to support the following functions: maintain a history file (also called an Audit Log) that records all security-related events pertinent to establishing an audit trail for a "post-mortem" analysis of a suspected security breach; ensure integrity of the audit log; generate customized audit reports; protect audit log(s) from unauthorized access; support administrator-selectable alerts for specified security-related events; and support audit records of administrative events.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.7: Data Disposal<sup>9</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.7.1	Required	
2.7.2	Required	
2.7.3	Required	

## 2.8 System Integrity

This feature is focused on the functional integrity of the system, including the controlled creation, installation and operation of the system software and data. The security-related requirements in relation to system integrity include the following:

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.8: System Integrity<sup>10</sup></b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.8.1	Required	
2.8.2	Required	
2.8.3	Required	
2.8.4	Required	
2.8.5	Required	
2.8.6	Required	

<sup>9</sup> "Data disposal" is defined as: The system shall ensure that there is no residual data exposed to unauthorized users as resources are allocated to, or released from, those data objects.

<sup>10</sup> "System integrity" is defined as: The system shall offer features to support the following functions: perform integrity checks for system functions; retain the security parameters after the occurrence of events such as system restart, disaster recovery, and arrival of sensitive dates related to the Y2K issue; provide the back-up capability to restore the system, when necessary, to a well-defined state (such as the need to undo modifications to a file or to undo transactions); ensure that security features are always invoked and may not be bypassed unless authorized and configured to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.8: System Integrity<sup>10</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.8.7	Required	
2.8.8	Required	
2.8.9	Required	
2.8.10	Required	
2.8.11	Required	
2.8.12	Required	

## 2.9 Security Administration

This feature is focused on the required system capabilities and parameters that must be available to the administrator to operate and manage the system in a secure manner. The security-related requirements in relation to security administration include the following:

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.9: Security Administration<sup>11</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.9.1	Required	
2.9.2	Required	
2.9.3	Required	
2.9.4	Required	
2.9.5	Required	
2.9.6	Required	
2.9.7	Required	
2.9.8	Required	
2.9.9	Required	
2.9.10	Required	

## 2.10 Guidance

This feature is focused on the assurance aspect of system security by supplementing the technical security capabilities with appropriate direction on securely configuring, operating and managing the system. The security-related requirements in relation to guidance include the following:

---

<sup>11</sup> “Security administration” is defined as: The system shall offer features to selectively authorize a highly privileged user (a security administrator) to perform day-to-day activities such as: activate protective features (e.g., the login feature); customize (i.e., override, if appropriate) vendor-provided defaults; monitor suspected activities related to a potential security breach; detect security violation incidents promptly, isolate and investigate the problem, and securely recover the system; generate security audits when needed; and manage user accounts.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.10: Guidance<sup>12</sup></b> Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.10.1	Required	
2.10.2	Required	
2.10.2.1	Required	
2.10.2.2	Required	
2.10.2.3	Required	
2.10.2.4	Required	
2.10.2.5	Required	
2.10.2.6	Required	
2.10.2.7	Required	
2.10.2.8	Required	
2.10.2.9	Required	

## 2.11 Non-Repudiation

This feature is focused on the system's capabilities for preventing users from denying their actions in terms of sending or receiving data.

---

<sup>12</sup> "Guidance" is defined as: The vendor shall supply the following product support capability: a cogent security-related document for administration (e.g., a "Security Administration Guide") that would be made available as a hard copy or an electronic file, as an entity unto itself, and not fragmented throughout the reference manuals; a cogent user guide for security functions that would provide guidance for configuring the product's security features and maintaining security on an ongoing basis.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.11: Non-repudiation<sup>13</sup> (DESIRED)</b>		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
NOTE: The classification of “DESIRED” here means that if the product submitted for evaluation does not provide non-repudiation functions, then it need not comply with the criteria in this section. However, if the product submitted for evaluation claims to provide non-repudiation functions, it must fully comply with items 2.11.1 – 2.11.3.		
2.11.1	Required	<i>See NOTE above.</i>
2.11.2	Required	<i>See NOTE above.</i>
2.11.3	Required	<i>See NOTE above.</i>

### 3. Product Functionality

This section of the criteria refers to the primary functionality of the product and how it is affected by security. For products whose primary functionality is not security (e.g., applications, databases, operating systems, etc.), this section will test how that functionality is impacted by the security features of the product, as described in Section 2 of the Criteria. However, for those products whose primary functionality is security-related (e.g., authentication systems, network security products, authorization systems, etc.), the “functionality” criteria will address the main purpose of the product. In the cases of these product profiles, the “functionality” section of the criteria will often be as detailed, if not more so, than the “security features” section. Furthermore, since the Product Profiles address a wide variety of products within a class, it is permissible for the Profile to contain functionality criteria specific to a “subclass” of products (e.g., the Authentication Systems profile might contain criteria specific to biometrics systems, smart cards, PKI, etc.).

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
3.1	Required	

<sup>13</sup> “Non-repudiation” is defined as: The system shall have the capability of preventing users from successfully denying actions and events of users acting in the role of a sender or receiver.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
3.2	Required	

#### 4. Scalability

Scalability criteria shall specify minimum limitations in terms of traffic/use parameters of volume, frequency or time. These criteria are used to assess the degree to which security service objectives are met at or near system capacities or across multiple platforms. The focus of the testing shall be to verify vendor claims of the scalability of the product in a standard configuration. The criteria are applied in tests that are designed to stress the product design and to determine that the product retains security functionality as the offered traffic exceeds stated system capacities.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
4.1	Required	

## 3. Required Functional Criteria for Network Security Products

---

### 3.1 Introduction

This section lists the required criteria for the functional areas that are common to all products in this profile. Some subclasses of products will have additional, unique functionality for which additional required criteria will be listed separately in Section 5.

*Rationale* statements will be applied where appropriate.

The following functional criteria groups are provided:

- Access Mediation
- User Management
- Resource Management
- Entitlement Management
- Storage of Security Data
- Systems Management and Configuration
- Application Integration and Communications

It may be that the composition of a particular firewall, VPN or encryption product does not operate on an application (OSI model) or end-user level. However, users who are administrators or provide support and maintenance for the network security product are operators within or upon the network security product, are users of the system, and are governed by these criteria.

Similarly, not all network security products have functional operations related to the functional criteria groups provided here. In these instances, it will be obvious that particular criteria will not apply to a particular firewall, VPN or encryption product.

For example, some network security products may have objectives that are realized without permitting or denying access to controlled resources.

### 3.2 Access Mediation

Within the context of this product profile, “access mediation” is defined as the “runtime” decisions carried out by the system to determine resource access, and subsequently, permit or deny resource access for a requestor.

The access mediation feature is focused on the system functions and actions associated with the *granting* or *denial* of access to a resource in response to an access request. Access mediation is not concerned with the system functions associated with *establishing* access to an object. The security-related requirements in relation to access mediation include the following:

<b>CRITERIA</b>	<b>RATIONALE</b>
<p>3.2.1 The system shall provide the capability to require authentication of users to establish system access based on administrator-specified parameters.</p>	<p><i>It is essential that the system only permit access to objects by identified and authenticated users of the system. Without this criterion, audit activity and assignment of permissions to protected resources is not possible.</i></p> <p><i>Resources, as used in this criterion, refers to resources protected by the network security product and the resources that the network security product is composed of or offers for use.</i></p>
<p>3.2.2 If the product supports a distributed (manager/agent) model for access control:</p> <ul style="list-style-type: none"> <li>• Privileges on “target platforms”<sup>14</sup> must be accordant with access administration policies maintained in the main/central repository. The system must provide a facility that ensures that a user’s access and privileges on target platforms are the same as access policies in the central repository.</li> </ul>	<p><i>It is essential that target platforms reflect the access and privilege status intended and established by the administrator. Security settings that do not reflect the intent of the administrator suggest product instability and can lead to unintended security breaches.</i></p>
<p>3.2.3 The network security system shall have the capability to restrict session establishment based on the source of the connection.</p>	
<p>3.2.4 The systems shall provide sufficient checks on data and commands from every source. The systems shall reject data that fails all criteria.</p>	<p><i>As data sources may be only semi-trusted, it is imperative that a system not make assumptions about the source’s data integrity. By forcing criteria checks on data, the system will significantly reduce the chances of malformed, bogus or malicious data from corrupting the system or exploiting a hole in the core design.</i></p>
<p>3.2.5 The systems shall require explicit authorization to perform the following:</p> <ul style="list-style-type: none"> <li>• Accept downloads from a server or client</li> <li>• Run scripts</li> </ul>	

<sup>14</sup> Target Platforms are those platforms under administrative interface to main management consoles via “agents.”

<i>CRITERIA</i>	<i>RATIONALE</i>
<ul style="list-style-type: none"> <li>• Enable executables</li> </ul>	
3.2.6 The systems shall have the capability to filter data relayed through any interface. The systems shall reject data that allows for unauthorized or malicious system calls.	

### 3.3 User Management

Within the context of this product profile, “user management” is defined as the administrator activity of defining, adding, changing and deleting user-IDs, accounts and associated parameters.

User management is focused on the system functions and actions associated with establishing user-IDs and accounts within the system. It also encompasses any security-related parameters that can be defined, changed or deleted to manage and configure the IDs and accounts. The security-related requirements in relation to access mediation include the following:

<i>CRITERIA</i>	<i>RATIONALE</i>
3.3.1. The system shall support the ability to delete or disable any user-IDs, including pre-defined vendor-supplied and/or system defaults.	<i>For pre-defined default user-IDs in particular, a facility must be available to nullify pre-defined default user-IDs because these IDs are typically targeted by attackers.</i>
3.3.2. The system shall support separate user-IDs for every administrator and operator of the system.	<i>Without separate user-IDs for all users of the system, accountability is lost. For example, if IDs are shared, there is no way to determine who performed an action.</i>
3.3.3. The system shall not allow a user to invoke any function or process (except the login process) without an appropriately privileged user-ID.	
3.3.4. The system should allow for separate authentication processes for administrators and privileged users.	<i>Each individual user must have associated authentication information to ensure the authenticity and integrity of the user's identity.</i>
3.3.5. When a system manager is a product component, it shall maintain explicit user authentication when the application is accessed across a proxy-based interface.	

### 3.4 Storage of Security Data

Within the context of this product profile, “storage of security data” is defined as administrator activities regarding the secure storage of data for reasons such as confidentiality, audit and non-repudiation. The security-related requirements in relation to storage of security data include the following:

<i>CRITERIA</i>	<i>RATIONALE</i>
3.4.1 If the product supports a distributed (manager/agent) model for access control: <ul style="list-style-type: none"> <li>When the system identifies discrepancies between central repositories and target platforms, the system shall send notification (e.g., an email message) to the administrators for resolution within an administrator-configured time and disable the access on the target platforms.</li> </ul>	<i>When target platforms do not reflect the access and privilege status intended and established by the administrator, it is essential that the administrator be notified of the discrepancy. Notification enables prompt corrective response by the administrator.</i>
3.4.2 If the network security product supports a distributed (manager/agent) model for user-ID and account management: <ul style="list-style-type: none"> <li>When the system identifies discrepancies between central repositories and target platforms, the system shall send notification (e.g., an email message) to the administrators for resolution within an administrator-configured time period and disable the access on the target platforms.</li> </ul>	<i>When target platforms do not reflect the user-ID and account privilege status intended and established by the administrator, it is essential that the administrator be notified of the discrepancy. Notification enables prompt corrective response by the administrator.</i>

### 3.5 Systems Management and Configuration

<i>CRITERIA</i>	<i>RATIONALE</i>
3.5.1. The system shall not negatively impact the integrity of the underlying platform and supporting infrastructure.	<i>It is essential that the system ensure the integrity of data maintained within a system, as well as the underlying platform and supporting infrastructure.</i>
3.5.2. The system management component of the product shall have the capability to support the security administrator’s role to configure the security-relevant options.	

<b>CRITERIA</b>	<b>RATIONALE</b>
3.5.3. When a system manager is a product component, it shall limit the ability to make changes to security-relevant options and user security capabilities to an appropriately privileged user or administrator.	
3.5.4. The system shall provide a Security Administration Guide that documents the process for securely configuring and maintaining the security capabilities of the system by the administrator.	<i>The importance of a Security Administration Guide is directly associated with the competency of the administrator and the resulting implementation of the security system. Consequently, an administration guide improves security.</i>
3.5.5. The systems shall provide the security functions in a consistent manner.	<i>For example, the terminology used in various administration screens should be consistent.</i>

## 4. Desired Functional Criteria for Network Security Products

### 4.1 Introduction

This section will list the optional criteria for the functional areas that are common to all products in this profile. Some subclasses of products will have additional, unique functionality for which additional *desired* criteria will be listed separately in Section 5.

Rationale statements will be applied where appropriate.

### 4.2 Product Configuration

	<i>CRITERIA</i>	<i>RATIONALE</i>
4.2.1	<b>DESIRED:</b> The system should facilitate non-repudiation of transactions or communications by performing authentication of related parties and maintaining data integrity for related transactions or communications.	<i>Authentication and data integrity, in support of non-repudiation of transactions and communications, is an essential financial industry requirement. Without this ability, a transaction or communication cannot be proven and confirmed.</i>  <i>This facility shall provide the ability to verify that a specific communication or transaction originated with, was submitted by, or was delivered to a certain party.</i>
4.2.2	<b>DESIRED:</b> When a system manager is a product component, the management application should restrict private data received from one client application from being accessed by another client application	
4.2.3	<b>DESIRED:</b> The system should have the capability to interface with industry standard security and directory services.	<i>The system will need to integrate with typical third-party security products such as ldap, smnp, etc.</i>
4.2.4	<b>DESIRED:</b> This product should provide interfaces that would allow third-party products to integrate with it.	
4.2.5	<b>DESIRED:</b> When a system manager is a product component, if the manager stays constantly logged onto another system on a long-term basis (e.g., continuous session), the application should support periodic re-authentication of the connection.	<i>This should help to prevent session hijacking.</i>

<b>CRITERIA</b>		<b>RATIONALE</b>
4.2.6	<b>DESIRED:</b> A system should provide an administrator, as authorized, with the capability to independently and selectively monitor (in real time) the actions of any user currently logged on and lock out that user if necessary.	<i>This provides the administrator with the capability to monitor actions on the system, in support of the ability to monitor unauthorized activity. This capability is often used in “honey-pots” and other forensic activity.</i>
4.2.7	<b>DESIRED:</b> A system should provide an administrator, as authorized, with the capability to independently and selectively monitor (in real time) the activities at a specified terminal, port or network address, and lock out that input device if necessary.	<i>Just as the administrator requires the ability to monitor activities of a specific user, the same is true of activities of a specific connection.</i>
4.2.8	<b>DESIRED:</b> The system should have the capability to archive security related events.	<i>Having the capability to archive audit event logs is beneficial as a forensic analysis tool that can help determine the root cause of an incident. An archive will enable this capability long after an incident has occurred.</i>
4.2.9.	<b>DESIRED:</b> The system should support a capability for the administrator to configure the presentation of appropriate administration-relevant alerts and dialog displays for security-related events such as: <ul style="list-style-type: none"> <li>• Acceptance of data from the remote clients or server applications</li> <li>• Changes in security modes including rollback attacks and failures</li> <li>• Sending data over untrusted communications connections</li> </ul>	<i>Overall security benefits improve when the system provides the capability for the administrator to tailor the system security information in a format that enables more efficient and thorough monitoring.</i>
4.2.10.	<b>DESIRED:</b> The systems should support authentication for process-to-process communication.	<i>Remote method invocation example – SOAP (SSL)</i>

## 5. Functional Criteria for Network Security Systems Product Sub-classes

---

### 5.1 Introduction

For each of the subclasses listed below, this section lists the minimal functionality in terms of functional criteria expected in products of that subclass.

#### ***Firewall Products***

Firewalls focus on restricting network traffic according to a security policy. The most basic means of restricting network traffic is with a TCP/IP address and TCP/IP port number. This is the functionality provided by traditional packet filters. Modern firewalls provide many ways to improve upon basic packet filters. Many methods have been applied to enable firewalls to more completely secure a great variety of applications and services. Most existing firewalls can recognize many application types and the characteristics of each application.

In addition, some firewalls have the capability to provide Virtual Private Network (VPN) services while also functioning as a firewall.

#### ***Virtual Private Network (VPN) Products***

Virtual private networks (VPN) provide secure communications across unsecured media such as the Internet. The VPN can be a link between sites, which is provided by a dedicated system at each site. A VPN can also be established between remote users and various corporate sites. The device that provides the VPN is, ideally, dedicated to the task of providing VPN services.

A VPN is a wide area communications network provided by a common carrier that provides what seems like dedicated lines when used, but instead shares backbone trunks among all customers as in a public network. It allows a private network to be configured within a public network.

If a product comes bundled with VPN, the VPN features or functionality must also meet the criteria listed in the VPN section.

#### ***Link Layer Encryption Products***

Link-Layer encryption products are systems operating, typically, in a leased-line, frame relay, ATM network or point-to-point arrangement performing networking security at the OSI layer-1 or 2 level. These products will focus on criteria supporting these characteristics and are

exclusive of criteria for “network-to-network” encryption product types within the VPN subsection.

Data traversing unsecured networks is subject to many kinds of threats. Data can be read, altered or forged by anyone with access to the route the data takes. For example, a protocol analyzer can read packets and access confidential information.

Encryption can provide a means to safeguard network data that travels from one host or device to another across unsecured networks. Encryption is particularly important if confidential or critical data is being transmitted

## 5.2 Functional Criteria for Firewall Products

<i>CRITERIA</i>	<i>RATIONALE</i>
5.2.1 If the firewall system comes bundled with a VPN solution, the product shall provide an administrator-configurable option to enable VPN clients to securely access the private enterprise network.	
5.2.2 The firewall product shall provide the administrator with the capability to define URLs to control access to websites.	
5.2.3 When the firewall provides authentication controls, it shall also permit and facilitate configurable authentication databases.	<i>The firewall should be configurable to authenticate using, for example, a local list, LDAP server, Radius server, NDS, NT, etc.</i>
5.2.4 For products supporting user name accounts, the firewall product shall provide an administrator-configurable option to enable a username lookup and then logging of a username, group and domain name on the firewall.	

<i>CRITERIA</i>	<i>RATIONALE</i>
5.2.5 The firewall product shall provide a feature to mitigate network-level denial of service attacks.	<i>If, for example, the firewall is able to intercept packets and examine them for the patterns common to SYN flood attacks, then the firewall can protect the system from this denial-of-service attack. Additionally, if every SYN packet is intercepted and responded to by the firewall on behalf of the server with a SYN/ACK segment, the firewall retains state information and waits for the client's acknowledgement. When the ACK is received, the TCP three-way handshake is performed between the firewall and the server, and the connection can resume as normal.</i>
5.2.6 The firewall product shall provide a feature to prevent or control IP spoofing.	<i>Reverse route lookups are a good way to prevent IP spoofing attacks. Firewall functionality that enables screening of inbound packets that arrive on select interfaces to determine the integrity of the IP source can mitigate IP spoofing.</i>
5.2.7 The firewall product shall ensure that only authorized administrators can configure firewall rules.	
5.2.8 If the product supports application-based proxies, the firewall product shall provide full support for defining new proxies and the ability to implement rule sets for them.	<i>This would be tested by looking at the extent of provided proxies, as well as the ability to create new proxies.</i>
5.2.9 The firewall product shall provide the ability to notify the product administrator of conflicts or rules that will not be used, when a rule is created or changed.	
5.2.10 <b>DESIRED:</b> The firewall product should provide the ability to log activity, specified events and specified information related to product usage.	
5.2.11 <b>DESIRED:</b> The firewall product should provide the ability to record and display rule creation history and rationale.	
5.2.12 <b>DESIRED:</b> An added feature would be the ability to control entire groups of URLs based on full or partial text string matches within URLs.	

<b>CRITERIA</b>	<b>RATIONALE</b>
5.2.13 <b>DESIRED:</b> The firewall product should provide an administrator-configurable option to enable authentication and permissions based on identification, source IP address or some set of parameters.	
5.2.14 <b>DESIRED:</b> The firewall product should have features that support content inspection capabilities to block or control content based on site security policy.	
5.2.15 <b>DESIRED:</b> The firewall product should provide content filtering features that support anti-virus technologies, including scanning and removal of viruses and detailed logging events.	
5.2.16 <b>DESIRED:</b> The firewall product should provide a database of rules with descriptive text information.	<i>Being able to record and store information describing the business reason for the rule will assist in setting, changing or analyzing rules for a firewall product.</i>

### 5.3 Functional Criteria for Virtual Private Network (VPN) Products

<b>CRITERIA</b>	<b>RATIONALE</b>
5.3.1 When the VPN product provides authentication controls, it shall also permit and facilitate configurable authentication databases.	
5.3.2 The VPN product shall enable administrators to control and establish the authorized users of the VPN and the user-accessible network resources.	
5.3.3 The VPN product shall provide the capability to remotely manage multiple systems or multiple remote access clients.	
5.3.4 The VPN product shall enable and support standards-based encryption algorithms and methods.	<i>See Appendix A.</i>
5.3.5 The VPN product shall enable and support standards-based authentication algorithms and methods.	<i>See Appendix A.</i>

<b>CRITERIA</b>	<b>RATIONALE</b>
5.3.6 The VPN product shall enable and support standards-based key management protocols and methods.	<i>See Appendix A.</i>
5.3.7 The VPN product shall allow for the online registration of users and the distribution of the VPN client software to users.	
5.3.8 For remote access, the VPN product shall enable or facilitate the management of multiple VPN servers or appliances from a single location and from multiple locations.	
5.3.9 The VPN product shall protect the authentication information that is in its possession.	<i>In cases where the VPN is being used by an automated process (e.g., server to server).</i>
5.3.10 The VPN product shall provide the ability to restrict sessions to explicitly authorized IP addresses and ports.	
5.3.11 The VPN product shall allow encryption of a network protocol other than IP through encapsulation of the protocol within an IP packet	
5.3.12 The VPN product or device shall enable IP packet encryption or decryption only if the packet meets administrator configurable parameters.	<i>This capability allows the enterprise, through administrator-only configuration parameters, to selectively determine via individual packets which IP addresses or networks will enforce encryption.</i>
5.3.13 The VPN product shall provide the capability to periodically renegotiate or perform a key exchange for a new session keybased on an administrator-configurable parameter(s) such as “key timeout” settings or volume of data.	
5.3.14 The VPN product shall ensure that peer sites or devices successfully authenticate each other. If either authentication fails, the encrypted session must not be established.	<i>Peer authentication ensures that only known, trusted peer devices exchange encrypted traffic, and prevents routers from being tricked into sending sensitive encrypted traffic to illegitimate or fraudulent destination devices.</i>

<b>CRITERIA</b>	<b>RATIONALE</b>
<p>5.3.15 <b>DESIRED:</b> The VPN product should provide the capability to validate public keys. The generated keys should be used to mutually authenticate the peers during session establishment and to exchange session keys.</p>	<p><i>An encrypted session must be established before a device can send encrypted data to a peer device. An encrypted session is established whenever a device detects an IP packet that should be encrypted and no encrypted session already exists.</i></p> <p><i>To establish a session, two peers exchange connection messages. The primary purpose is to authenticate each router to the other. The secondary purpose of the connection messages is to generate a temporary DES key ("session key"), which is the key that will be used to actually encrypt data during the encrypted session.</i></p>
<p>5.3.16 <b>DESIRED:</b> The VPN product should provide or support the administrator configurable use of multiple access control methods.</p>	<p><i>Examples are radius, TACACS, local proxy rules and digital certificates.</i></p>
<p>5.3.17 <b>DESIRED:</b> The VPN product should provide, based upon the administrator's specification, the ability to secure a client while the VPN is in use.</p>	<p><i>For example, if the VPN is used to secure remote client access to a network over the Internet, there is a risk that the client PC will be attacked while it is connected to the Internet, especially when a DSL or cable connection is used. The VPN product should allow the administrator to specify security requirements for VPN clients such that all Internet connections on the client, outside of those initiated by the user through the VPN, are refused while the VPN session is in process.</i></p>
<p>5.3.18 <b>DESIRED:</b> The VPN product should provide or support the administrator-configurable use of multiple authentication methods.</p>	<p><i>For example, Radius, TACACS, local database rules, user ID and password, smart card and token.</i></p>
<p>5.3.19 <b>DESIRED:</b> When private keys are stored within the VPN product, they should be stored in a secure and private manner, where they cannot be viewed in any way, including system commands. Otherwise, private keys are stored within a secure removable storage media such as a smart card or SmartToken.</p>	<p><i>When an encrypted session is being established, each device uses the peer's DSS public key to authenticate the peer.</i></p>

## 5.4 Functional Criteria for Link Layer Encryption Products

<b>CRITERIA</b>	<b>RATIONALE</b>
-----------------	------------------

<i>CRITERIA</i>	<i>RATIONALE</i>
5.4.1. The link layer encryption product shall provide the capability to periodically renegotiate or perform a key exchange for a new session key based on an administrator-configurable parameter(s) such as “key timeout” settings or volume of data.	
5.4.2. The link layer encryption product shall ensure that peer sites or devices successfully authenticate each other. If either authentication fails, the encrypted session must not be established.	<i>Peer authentication ensures that only known and trusted peer devices exchange encrypted traffic, and prevents routers from being tricked into sending sensitive encrypted traffic to illegitimate or fraudulent destination devices.</i>
5.4.3. The link layer encryption product shall facilitate or enable standard encryption algorithms for data encryption and decryption. This capability shall be available to be employed in conjunction with other encryption controls.	<i>See Appendix A.</i>
5.4.4. The link layer encryption product shall support concurrent encrypted sessions with multiple destinations.	
5.4.5. <b>DESIRED:</b> The link layer encryption product should provide the capability to validate public keys. The generated keys should be used to mutually authenticate the peers during session establishment and to exchange session keys.	<p><i>An encrypted session must be established before a device can send encrypted data to a peer device. An encrypted session is established whenever a device detects an IP packet that should be encrypted, and no encrypted session already exists.</i></p> <p><i>To establish a session, two peers exchange connection messages. The primary purpose of the connection messages is to authenticate each router to the other. The secondary purpose is to generate a temporary DES key ("session key"), which is the key that will be used to actually encrypt data during the encrypted session.</i></p>
5.4.6. <b>DESIRED:</b> When private keys are stored within the link layer encryption product, they should be stored in a secure and private manner, which cannot be viewed in any way, including system commands. Otherwise, private keys are stored within a secure removable storage media such as a smart card or SmartToken.	<i>When an encrypted session is being established, each device uses the peer's DSS public key to authenticate the peer.</i>

## Appendix A: Industry Standards

For the purposes of these criteria, the terms “public and widely used standards” and “financial industry standards” shall refer to those standards, algorithms and protocols listed below, as well as other relevant standards approved by the following organizations: IETF, ANSI X9, ITU-T, ISO, NIST and IEEE.

Symmetric encryption algorithms	<ul style="list-style-type: none"> <li>• 3DES (ANS X9.52, X9.66)</li> <li>• IDEA</li> <li>• RC4</li> <li>• RC5</li> <li>• RIPEM</li> </ul>
Asymmetric algorithms (for symmetric key agreement or key transport)	<ul style="list-style-type: none"> <li>• RSA (ANS X9.44)</li> <li>• D-H (minimum 1024-bit modulus – ANSI X9.42)</li> <li>• ECDH (ANS X9.63)</li> <li>• Elliptic Curve</li> </ul>
Digital hashing algorithms	<ul style="list-style-type: none"> <li>• SHA-1 (ANS X9.30-2)</li> <li>• MD5</li> </ul>
Digital signature algorithms	<ul style="list-style-type: none"> <li>• DSA (ANS X9.30-1)</li> <li>• rDSA (ANS X9.31) (includes RSA)</li> <li>• EC-DSA (ANS X9.62)</li> </ul>
Key management standards and protocols	<ul style="list-style-type: none"> <li>• ANS X9.70, ANS X9.73, ANS X9.69, ANS X9.24, ANS X9.77</li> <li>• CMP</li> <li>• PKCS #7, #10</li> <li>• IETF PKIX standards</li> </ul>
Random number generators	<ul style="list-style-type: none"> <li>• ANS X9.82</li> </ul>
Prime number generators	<ul style="list-style-type: none"> <li>• ANSI X9.80</li> </ul>
Cryptographic device security	<ul style="list-style-type: none"> <li>• ANS X9.66</li> <li>• FIPS 140-2</li> </ul>
Peer entity authentication	<ul style="list-style-type: none"> <li>• ANS X9.72</li> <li>• FIPS 196</li> </ul>
PIN security	<ul style="list-style-type: none"> <li>• ANS X9.8, ANS X9.86, ANS X9.87</li> </ul>
Biometrics management and security	<ul style="list-style-type: none"> <li>• ANS X9.84</li> </ul>
Directory standards	<ul style="list-style-type: none"> <li>• X.500</li> <li>• LDAP v3</li> </ul>
TCP/IP integrity	<ul style="list-style-type: none"> <li>• IPsec</li> </ul>

The system shall use any of the algorithms listed above or others that are supported by any of the standards organizations listed above. If the system uses any other cryptographic algorithm, then it shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm.

## Appendix B: Bibliography

---

MSC            *Master Security Criteria (v3.0)*, BITS, October 2001

## Appendix C: Glossary of Terms

Definitions provided in this document came from various books and publications. Several of these sources are listed at the end of this section.

TERM	DEFINITION
<b>access control</b>	<i>A mechanism for limiting use of a resource to authorized users. [1]</i>
<b>account</b>	<i>In terms of a “user account,” an account is an established relationship between a user and a computer, network or information service.</i>
<b>active attack</b>	<i>An attack that results in an unauthorized state change, such as the manipulation of files or the addition of unauthorized files. [3]</i>
<b>administrator</b>	<i>In the context of this profile and if used without pre-qualification, this term indicates any user or group of users that could be defined as being a system administrator and/or product administrator, typically having privilege beyond the scope of an end user. See also “end user,” “user” and “product administrator.”</i>
<b>automated information system (AIS)</b>	<i>Any interconnected system equipment or subsystems of equipment that are used in the automatic acquisition, storage, manipulation, control, display, transmission or reception of data, including software, firmware and hardware. [3]</i>
<b>american National Standards Institute (ANSI)</b>	<i>One of several organizations that develop and publish standards for computer networking. [1]</i>
<b>application programming interface (API)</b>	<i>An interface typically provided by a software development toolkit.</i>
<b>asymmetric cryptography</b>	<i>A class of cryptographic algorithms that use separate keys for encryption and decryption. [2]</i>
<b>attack</b>	<i>An attempt to bypass security controls on a computer. The attack may alter, release or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures. [3]</i>
<b>audit</b>	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
<b>authenticate</b>	<i>To determine that something is genuine. To reliably determine the identity of a communicating party. [1]</i>
<b>authentication</b>	<i>The process of reliably determining the identity of a communicating party. [1]</i>
<b>authenticator</b>	<i>The method, material or credential used to create and/or implement authentication bindings, such as a password, PIN number, token seed or smart card seed.</i>
<b>authorization</b>	<i>Permission to access a resource. [1]</i>
<b>biometric device</b>	<i>A device that authenticates people by measuring some hard-to-forge physical property, like a fingerprint or the strokes and timing of a signature.</i>
<b>biometrics</b>	<i>Using physical characteristics of users such as fingerprints and retinal impressions to authenticate users. [2]</i>
<b>buffer overflow</b>	<i>When more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes, and can result in system crashes or the creation of a back door leading to system access [3]</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>certificate</b>	<i>A message signed with a public key digital signature stating that a specified public key belongs to someone or something with a specified name. [1]</i>
<b>certificate authority (CA)</b>	<i>Something trusted to sign certificates. [1]</i>
<b>certificate revocation list (CRL)</b>	<i>A list of names of users and roles that are no longer valid within a public key cryptography system. [2]</i>
<b>challenge-response</b>	<i>An authentication mechanism in which the authentication process sends a challenge to a process that requests authentication; the latter is authenticated only if it sends the correct response to the authentication process. [2]</i>
<b>clear text</b>	<i>A message or data that is not encrypted.</i>
<b>client</b>	<i>Something that accesses a service by communicating with it via a computer network. [1]</i>
<b>confidentiality</b>	<i>The property of not being divulged to unauthorized parties. [1]</i>
<b>credential</b>	<i>A letter or certificate given to a person to show that he or she has a right to confidence or to the exercise of a certain position or authority. [5]</i>
<b>cryptography</b>	<i>The practice of encoding and decoding data.</i>
<b>decrypt</b>	<i>To undo the encryption process. [1]</i>
<b>dictionary attack</b>	<i>An attack in which the attacker “guesses” passwords based on a set of key words or characters until a match is made. Also called an “offline attack” or “brute force attack.”</i>
<b>digital signature</b>	<i>A method based on public key encryption to verify identities over a network.</i>
<b>distributed system</b>	<i>Multiple systems and/or processors that are working to support one set of applications or functions, even from geographically disperse locations.</i>
<b>dynamic link library (DLL)</b>	<i>Software (executable code or data, such as icons or fonts) used by Microsoft Windows and IBM's OS/2 to provide services (such as a LAN driver or a distributed filing system) to applications. One memory-resident copy of the DLL can be simultaneously shared by all applications.</i>
<b>domain name system (DNS)</b>	<i>An Internet service that translates domain names into IP addresses.</i>
<b>dongle</b>	<i>A device that attaches to a computer to control access to a particular application.</i>
<b>encrypt</b>	<i>To scramble information so that only someone who knows the appropriate secret can obtain the original information (through decryption).</i>
<b>end user</b>	<i>In the context of this profile and unless otherwise indicated, this term will be associated with the end user of the product. See also “user” and “administrator.”</i>
<b>engine</b>	<i>In the context of this profile and unless otherwise indicated, this term will be associated with the systems that are accessed and possibly controlled by the management system. See also “manager.”</i>
<b>escrow</b>	<i>To hold something in safekeeping. Most uses of the word imply keeping something safe from the owner, as opposed to providing any safety for the owner.</i>
<b>engine</b>	<i>In the context of this profile and unless otherwise indicated, this term will be associated with the systems that are accessed and possibly controlled by the management system. See also “manager.”</i>
<b>Federal Information Processing Standard (FIPS)</b>	<i>One of a series of U.S. government documents that specifies standards for various aspects of data processing, including the Data Encryption Standard (DES). [1]</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>group</b>	<i>A named collection of users created for convenience in stating authorization policy.</i>
<b>hash</b>	<i>A cryptographic one-way function that takes an arbitrary-sized input and yields a fixed-size output. [1]</i>
<b>immutable</b>	<i>Unchangeable. [2]</i>
<b>integrity</b>	<i>The quality of being uncorrupted. Message integrity refers to the state of a message not being modified while in transit. File integrity refers to the state of files not being modified while in storage. [2]</i>
<b>interface</b>	<i>In the context of this document, the term “interface” represents a separate entry point into the system. The term “interface” (i.e., “user interface”) is defined in the context of product administration, indicating the entry point for commands and menu(s) to a system.</i>
<b>international data encryption algorithm (IDEA)</b>	<i>A secret key cryptographic scheme. [1]</i>
<b>international Standards Organization (ISO)</b>	<i>A worldwide federation of national standards bodies from approximately 130 countries. In the context of this document, an ISO reference will focus on work in the field of information technology, as carried out by a joint ISO/IEC technical committee (JTC 1). (Also called the International Organization for Standardization.)</i>
<b>internet Engineering Task Force (IETF)</b>	<i>A standards body that focuses on protocols for use in the Internet. Its publications are called Internet RFCs (Requests for Comment). [1]</i>
<b>intrusion Detection Systems (IDS)</b>	<i>Techniques for detecting intrusion into a computer or network by observation of actions, security logs or audit data. Break-ins or break-in attempts are either detected manually or via software expert systems that operate on logs or other information available on the network.</i>
<b>key</b>	<i>A quantity used in cryptography to encrypt or decrypt information.</i>
<b>key escrow</b>	<i>The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees. [3]</i>
<b>log</b>	<i>To record an action. [2]</i>
<b>log file</b>	<i>A file that lists actions that have occurred. [2]</i>
<b>message authentication code (MAC)</b>	<i>A synonym of message integrity code (MIC). [1]</i>
<b>manager</b>	<i>In the context of this profile and unless otherwise indicated, this term is associated with the management system and supporting hardware and software. See also “engine.”</i>
<b>message digest</b>	<i>An irreversible function that takes an arbitrary sized message and outputs a fixed length quantity. MD2, MD4 and MD5 are message digest algorithms. [1]</i>
<b>multifactor</b>	<i>More than two elements or quantities.</i>
<b>message integrity code (MIC)</b>	<i>A fixed-length quantity generated cryptographically and associated with a message to reassure the recipient that the message is genuine. [1]</i>
<b>NIST</b>	<i>National Institute of Standards and Technology</i>
<b>non-repudiation</b>	<i>The property of a scheme in which there is proof of who sent a message, that a recipient can show to a third party who can independently verify the source [1]</i>

TERM	DEFINITION
<b>network time protocol (NTP)</b>	<i>A facility that allows for synchronized timekeeping among a set of distributed time servers and clients. It is a standard protocol that enables client computers to maintain system time synchronization to the US Naval Observatory Master Clocks. NTP runs as an application program, and it sends periodic time requests to one or more servers, obtaining server timestamps and using them to adjust the client's clock.</i>
<b>online certificate status protocol (OCSP)</b>	<i>Facilitates determining the current status of a digital certificate. It enables applications to determine the revocation status of a certificate. OCSP may provide more timely and accurate revocation information than is possible with Certificate Revocation Lists.</i>
<b>offline attack</b>	<i>An attack performed while offline to the system being attacked (see also “dictionary attack”).</i>
<b>one-time passwords</b>	<i>Passwords that can only be used once. [2]</i>
<b>operator</b>	<i>In the context of this profile, “operator” maintains similar relationships and functions as “administrator” (see above), given different and/or additional privileges than a typical “end user” of a system.</i>
<b>orthogonal</b>	<i>Having to do with right angles; rectangular. [5]</i>
<b>packet filters</b>	<i>Packet filters keep out certain data packets based on their service type and source and destination addresses. Filters can be used to block connections from or to specific hosts, networks or ports. Packet filters are simple and fast.</i>
<b>passive attack</b>	<i>An attack that does not result in an unauthorized state change, such as an attack that only monitors and/or records data. [3]</i>
<b>password</b>	<i>A supposedly secret string used to prove one's identity. [1]</i>
<b>personal identification number (PIN)</b>	<i>A short sequence of digits used as a password. [1]</i>
<b>public key cryptography standards (PKCS)</b>	<i>A set of standards, first introduced in 1991 by RSA Data Security, Inc., for implementing public key cryptographic algorithms and incorporating them in to applications. [2]</i>
<b>plaintext</b>	<i>Unencrypted data. [3]</i>
<b>port number</b>	<p><i>A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers, and physically between the transport layer and the Internet Protocol layer and forwarded on.</i></p> <p><i>Some services or processes have conventionally assigned permanent port numbers. These are known as “well-known port numbers.” In other cases, a port number is assigned temporarily (for the duration of the request and its completion) from a range of assigned port numbers. This is called an “ephemeral port number.”</i></p>
<b>pre-authentication</b>	<i>A protocol for proving you know your password before you are allowed access to a high quality secret encrypted with that password. [1].</i>
<b>private key</b>	<i>The quantity in public key cryptography that must be kept secret. [1]</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>privileged user</b>	<i>A user of a computer or system who is authorized to bypass normal access control mechanisms, usually in order to be able to perform system management functions. [1]</i>
<b>product administrator</b>	<i>In the scope of this profile, this role is associated with a user having higher privilege at the product's configuration level. This user (role) may be the same as that of the system administrator, but could also be different.</i>
<b>protected path</b>	<i>A mechanism that guarantees a mutually authenticated channel. [4]</i>
<b>public key</b>	<i>The quantity in public key cryptography that is safely divulged to as large an extent as is necessary or convenient. [1]</i>
<b>public key cryptography</b>	<i>A cryptographic system where encryption and decryption are performed using different keys. (See asymmetric key cryptography.) [2]</i>
<b>relying party</b>	<i>In the scope of this profile, "relying party" is typically associated with the use of "system" (see below). It is associated frequently with the extent to which a criteria is in scope, as in references to an application or component maintaining reliance on another element to support said criteria.</i>
<b>replaying</b>	<i>Storing and retransmitting messages; the word is usually used to imply that the entity that replies to messages is mounting some sort of security attack.</i>
<b>repudiation</b>	<i>Denying that one did something or made some statement. [1]</i>
<b>resource</b>	<i>As referred to in these criteria, a resource includes resources protected by the security product, offered for use by the security product, and that comprise the security product.</i>
<b>revoke</b>	<i>To withdraw, repeal, rescind, cancel or annul. [5]</i>
<b>role</b>	<i>A function or office assumed by someone. [5]</i>
<b>security domains</b>	<i>The sets of objects that a subject has the ability to access. [3]</i>
<b>security features</b>	<i>The security-related functions, mechanisms and characteristics of AIS hardware and software. [3]</i>
<b>server</b>	<i>A resource available on the network to provide a service, such as name lookup, file storage or printing. [1]</i>
<b>sign</b>	<i>To use your private key to generate a digital signature as a means of proving you generated, or approve of, a message.</i>
<b>signature</b>	<i>A quantity associated with a message that only someone with knowledge of your private key could have generated, but that can be verified through knowledge of your public key. [1]</i>
<b>simple network management protocol (SNMP)</b>	<i>A simple composed set of network communication specifications that cover all of the basics of network management via a method that poses little stress on an existing network. Examples of these devices include routers, hubs and switches.</i>
<b>spoof</b>	<i>To convince someone that you are entity X when you are not, without X's permission. [1]</i>
<b>strong authentication</b>	<i>Authentication performed in such a way that it cannot easily be performed. Examples of strong authentication include one-time passwords, challenge-response mechanisms and cryptographic authentication. [2]</i>
<b>symmetric key cryptography</b>	<i>A class of cryptographic algorithms in which the same key is used for encryption and decryption. Examples of symmetric key algorithms include DES, IDEA, RC2, and RC4 [2]</i>

TERM	DEFINITION
<b>system</b>	<i>Within the scope of this profile, "system" is used to imply the totality of the product and the mediation device (if any) that need to be tested. [SCF 2.1.1]</i>
<b>system administrator</b>	<i>In the scope of this profile, an individual (user) who has higher privilege at the operating system level.</i>
<b>system recovery</b>	<i>Bringing a system from a down or inactive state to an operational and/or production state by reinstalling or repairing the underlying bios, operating system and/or related services and applications.</i>
<b>system restart</b>	<i>A shutdown and reloading of a system's bios, operating system and related services without interrupting power to the system (also known as a "warm boot").</i>
<b>transmission control protocol/Internet protocol (TCP/IP)</b>	<i>The common name for a family of more than 100 data communications protocols used to organize computers and data communications equipment into computer networks.</i>
<b>token device</b>	<i>A credit card sized device that generates authentication tokens, such as one-time passwords. [2]</i>
<b>two-factor authentication</b>	<i>A process in which two pieces of information are required to prove one's identity (such as a password and a smart card). [2]</i>
<b>weak authentication</b>	<i>Typically, this implies the conventional use of passwords.</i>
<b>user</b>	<i>In the context of this profile and if used without pre-qualification, this term indicates any and all users, such as end-user, product user-ID or system user.</i>
<b>user-ID</b>	<i>A number or name unique to a particular user of a computer or group of computers that share user information. The operating system uses the user-ID to represent the user in its data structures (e.g., the owner of a file or process or the person attempting to access a system resource)</i>
<b>X.509</b>	<i>A CCITT standard for security services within the X.500 directory services framework. The X.509 encoding of public key certificates has been widely adopted; the other protocol elements of X.509 have not. [1]</i>

**Glossary items are based on the following references:**

[1] Kaufman, C., Perlman, R. and Speciner, M., *Network Security: Private Communication in a Public World*, Prentice Hall, New Jersey, 1995

[2] Bernstein, T., Bhimani, A., Schultz, E., and Siegel, C., *Internet Security for Business*, John Wiley & Sons, Inc., New York, 1996

[3] NSA Glossary of Terms used in Security and Intrusion Detection

[4] Loscocco, Peter A., Smalley, Stephen D., Muckelbauer, Patrick A., Taylor, Ruth C., Turner, S. Jeff, Farrell, John F., *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments*, 1998

[5] Guralnik, David Bernard (editor), *Webster's New World Dictionary of the American Language*, 1986