
BITS Product Certification Program



Application Product Profile

Technical Contact Information

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

BITS Product Certification Program

bitslab@fsround.org

Tel. 202.289.4322

Fax: 202.289.3562

**Profile Leader/
Workgroup Chair:**

Sam Phillips, Senior Vice President, Bank of America

Roger Callahan, Senior Vice President, Bank of America

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

Representative	Organization	Representative	Organization
John Walsh	Allfirst Financial	Mike Foster	Wells Fargo
Eric Guerrino	Bank of New York	Garett Macey	Wells Fargo
Woody Tyner	BB&T Corporation	Fred Francis	Whitney National
Jim Strieber	BB&T Corporation	Rodney Chard	Whitney National
David Solo	Citigroup		
Steve Wyllie	FleetBoston Financial		
Howard Taylor	J.P. Morgan Chase		
Richard Yen	J.P. Morgan Chase		
Richard Feingold	Mellon Financial		
Jim Brown	Metavante Corporation		
Karla Warna	PNC Financial		
Landy Dutton	Regions Financial		
Steve Scott	Wachovia		
Keith Rodgers	Wells Fargo		

Profile Feedback

If you have any comments (technical or otherwise) regarding this profile, please send an email to bitslab@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, BITS will take all comments under advisement, but reserves the right to include or exclude comments received in the final criteria.*

Application Product Profile – Document Version Control History

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

Version / Date	Changes
1.0 (Aug 1999)	<ul style="list-style-type: none"> ◆ Initial Draft - internal distribution only
2.0 (Oct 1999)	<ul style="list-style-type: none"> ◆ BITS FSSL Application Product Profile Workgroup Distribution
3.1 (Dec 1999)	<ul style="list-style-type: none"> ◆ Initial “Open For Public Comment” Release
4.0 (Feb 2000)	<ul style="list-style-type: none"> ◆ <u>Page i</u>: “Profile Feedback” section added; Document Version Control History table added ◆ <u>Pages 1-2</u>: Rewrite of “Introduction” – New sections for “Overview”, “Boundaries and Underlying Platforms”, “Optional Criteria” and “Test Plans and Profiles” ◆ <u>ALL</u>: All Master Criteria references updated ◆ <u>Section 2.1.1</u> (Security Features, Identification): Items 4, 6 updated; Item 5 added ◆ <u>Section 2.1.2</u> (Security Features, Authentication): Added new outline numbers to sub groups ◆ <u>Section 2.1.2</u> (Security Features, Authentication, General Mechanism Requirements): Short description added; Items 2, 4 (orig. removed), 4, 7-8, 13-16 updated; (Knowledge/Possession-based Mechanism Requirements): Item 3 combined with Item 1 updated; Items 3, 7, 9, 11 updated; (Personal Characteristics-Based Mechanism Requirements): Items 1 updated; Items 2-3 added. ◆ <u>Section 2.1.3</u> (Security Features, Authorization): Items 3, 7 (new/inserted), 9-16, 18-19 updated; Item 24 removed ◆ <u>Section 2.1.4</u> (Security Features, Confidentiality): Items 3, 5-7, 9-12, 14 updated ◆ <u>Section 2.1.5</u> (Security Features, Data Integrity): Items 2, 10 (updated); Items 5, 16 (new/inserted) ◆ <u>Section 2.1.6</u> (Security Features, Audit): Items 2-9 (new/inserted) ◆ <u>Section 2.1.8</u> (Security Features, System Integrity): Item 2 (new/inserted) ◆ <u>Section 2.1.9</u> (Security Features, Security Administration): Item 2 (new/inserted) ◆ <u>Section 2.1.10</u> (Security Features, Guidance): Item 2 (new/inserted) ◆ <u>Section 2.1.11</u> (Security Features, Non-Repudiation): Item 1 (updated); Items 2-5 (new/inserted) ◆ <u>Section 2.2</u> (Functionality): Items 1 and 2 removed; New Item 1 inserted ◆ <u>Section 2.3</u> (Usability): Item 2 (new/inserted) ◆ <u>Section 2.4</u> (Scalability): Item 1 (updated) ◆ <u>Appendix A</u> (Industry Standards): new/inserted
5.0	<ul style="list-style-type: none"> ◆ <i>Re-formatted document</i> ◆ <i>Included new Master Security Criteria Version 3,0 criteria:</i> ◆ <i>Deleted section 3, 4 and 5. The working group decided that majority of the criteria that would be in sections 3,4, and 5 have already been addressed in section 2, at least for now.</i> ◆ <i>Updated Appendix A (Industry Standards)</i>

Version / Date	Changes
	◆ <i>Included Glossary of Terms</i>

Table of Contents

1. INTRODUCTION.....	1
2. CRITERIA FOR THE ADMINISTRATION AND OPERATION OF APPLICATION PRODUCTS	4
SECURITY FEATURES.....	4
3. PRODUCT FUNCTIONALITY.....	14
4. SCALABILITY.....	15
APPENDIX A: INDUSTRY STANDARDS.....	16
APPENDIX B: BIBLIOGRAPHY	17
APPENDIX C: GLOSSARY OF TERMS	18

1. Introduction

Overview

This Application Product Profile defines the security requirements to support the technical analysis of application systems. Examples of application systems include: electronic bill presentment and payment systems, funds transfer systems, personal finance managers, groupware and messaging systems, and web-based transaction systems, to name a few. The product profile identifies the criteria set, derived from the master criteria that apply to application systems. The criteria in the profile are applicable to the features and functions normally found in application systems.

For the purposes of this profile, the basic model for the application system is a client-server arrangement with the application interfacing with a browser or thin client, the underlying operating system and other entities using application program interfaces (APIs). This profile is focused on the application as implemented in a prototypical business environment and to assess its security dependencies on the underlying platform (e.g., operating system) and other remote entities (e.g., directories).

Mandatory and Desired Criteria

Each criterion will be identified as being *required* or *desired*¹. 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 Application Products”. 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.*

¹ A criterion shall be considered *required* unless it is explicitly identified as being *desired*.

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 product in this profile’s product class relies on the underlying operating system to provide scalable functionality. This configuration may be sufficient to meet the criteria within the profile for scalability. If, however, during the testing of the product (within this agreed-to testing boundary² and test plan), a vulnerability or issue is found in the operating system software that renders the system non-compliant with any of the test plan’s criteria test cases, the product will not earn the *BITS Tested Mark* unless the vulnerability or issue is addressed. This determination will be made regardless of the fact that the vulnerability may be in another vendor’s product, since it has been defined and agreed to as part of the test environment within the “boundary.”

Additionally, if the system uses any cryptographic algorithm not identified in Appendix A then the system shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm. Systems that do not have this flexibility will be disqualified from the BITS validation process.

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.*

Application 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).

² Reference: BITS Lab Testing Services Agreement (and Schedule A, Product Testing Schedule)

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
access control	<i>A mechanism for limiting use of some resource to authorized users. [1]</i>
audit	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
authentication	<i>The process of reliably determining the identity of a communicating party. [1]</i>
authenticator	<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>
confidentiality	<i>The property of not being divulged to unauthorized parties. [1]</i>
integrity	<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>
log file	<i>A file that lists actions that have occurred. [2]</i>
Master Security Criteria (MSC)	<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>
non-repudiation	<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>
privileged user	<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>
product administrator	<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>
system	<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>
system administrator	<i>In the scope of this profile, an individual (user) who has higher privilege at the operating system level.</i>
user-ID	<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 Application Products

Security Features

For each of the categories listed below, this section lists the minimal functionality in terms of security features expected in products of that category. 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 Application products. The criteria are categorized according to the following major sections in the Master Security Criteria.

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

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.1: Identification³		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise 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	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.2: Authentication⁴		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
Subsection 2.2.1: General Mechanism Requirements		
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	

³ "identification" is defined 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.

⁴ "Authentication" is identified 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
MSC Section 2.2: Authentication⁴ Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
2.2.1.6	Required	
2.2.1.7	Required	
2.2.1.8	Required	
Subsection 2.2.2: Knowledge and Possession-based Mechanism Requirements		
2.2.2.1	Required	
2.2.2.2	Required	
2.2.2.3	Required	
2.2.2.4	Required	
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	
Subsection 2.2.3: Personal Characteristics-Based Mechanism Requirements (DESIRED) Note: The classification of "DESIRED" for this entire subsection indicates the product submitted for evaluation may not need to comply with the criteria in this section. However, if the product is claiming to provide the capability it is <u>not</u> an optional section; it must fully comply with all criteria in this subsection (2.2.3).		
2.2.3.1	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>
2.2.3.2	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>
2.2.3.3	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.3: Authorization⁵ Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise 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	
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	
2.3.14	Required	
2.3.15	Required	
2.3.16	Required	
2.3.17	Required	
2.3.18	Required	

⁵ "Authorization" is identified as: The system shall offer features to support the following restrictions: no user shall be allowed access to the system without Identification and Authentication; 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
MSC Section 2.3: Authorization⁵		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
2.3.19	Required	
2.3.20	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.4: Confidentiality⁶		
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	
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	

⁶ "Confidentiality" is identified 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
MSC Section 2.5: Data Integrity⁷ 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	

⁷ "Data integrity" is identified 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
MSC Section 2.6: Audit⁸ 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	

⁸ “Audit” is identified 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; support audit records of administrative events.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.7: Data Disposal⁹		
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	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.8: System Integrity¹⁰		
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	
2.8.7	Required	
2.8.8	Required	
2.8.9	Required	

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

¹⁰ "System integrity" is identified 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, arrival of sensitive dates related to the Y2K issue, etc.; 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
MSC Section 2.8: System Integrity¹⁰		
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.		
2.8.10	Required	
2.8.11	Required	
2.8.12	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.9: Security Administration¹¹		
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	

¹¹ “Security administration” is identified 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
<p>MSC Section 2.9: Security Administration¹¹</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>		
2.9.10	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<p>MSC Section 2.10: Guidance¹²</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>		
NEW	DESIRED	<i>NEW CRITERIA¹³: The product should document any and all modifications performed by the product. This includes modifications to itself and to other components of the system.</i>
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	

¹² "Guidance" is identified 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.

¹³ All criteria identified as "New Criteria" in this section will be reviewed by the Financial Services MSC Committee for possible inclusion in a future release of the MSC.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
2.10.2.6	Required	
2.10.2.7	Required	
2.10.2.8	Required	
2.10.2.9	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.11: Non-repudiation¹⁴		
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	See NOTE above.
2.11.2	Required	See NOTE above.
2.11.3	Required	See NOTE above.

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

¹⁴ “Non-repudiation” is identified 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.

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	
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	

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

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
access control	<i>A mechanism for limiting use of a resource to authorized users. [1]</i>
account	<i>In terms of a “user account,” an account is an established relationship between a user and a computer, network or information service.</i>
active attack	<i>An attack that results in an unauthorized state change, such as the manipulation of files or the addition of unauthorized files. [3]</i>
administrator	<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>
automated information system (AIS)	<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>
american National Standards Institute (ANSI)	<i>One of several organizations that develop and publish standards for computer networking. [1]</i>
application programming interface (API)	<i>An interface typically provided by a software development toolkit.</i>
asymmetric cryptography	<i>A class of cryptographic algorithms that use separate keys for encryption and decryption. [2]</i>
attack	<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>
audit	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
authenticate	<i>To determine that something is genuine. To reliably determine the identity of a communicating party. [1]</i>
authentication	<i>The process of reliably determining the identity of a communicating party. [1]</i>
authenticator	<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>
authorization	<i>Permission to access a resource. [1]</i>
biometric device	<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>
biometrics	<i>Using physical characteristics of users such as fingerprints and retinal impressions to authenticate users. [2]</i>
buffer overflow	<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>
certificate	<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>

TERM	DEFINITION
certificate authority (CA)	<i>Something trusted to sign certificates. [1]</i>
certificate revocation list (CRL)	<i>A list of names of users and roles that are no longer valid within a public key cryptography system. [2]</i>
challenge-response	<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>
clear text	<i>A message or data that is not encrypted.</i>
client	<i>Something that accesses a service by communicating with it via a computer network. [1]</i>
confidentiality	<i>The property of not being divulged to unauthorized parties. [1]</i>
credential	<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>
cryptography	<i>The practice of encoding and decoding data.</i>
decrypt	<i>To undo the encryption process. [1]</i>
dictionary attack	<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>
digital signature	<i>A method based on public key encryption to verify identities over a network.</i>
distributed system	<i>Multiple systems and/or processors that are working to support one set of applications or functions, even from geographically disperse locations.</i>
dynamic link library (DLL)	<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>
domain name system (DNS)	<i>An Internet service that translates domain names into IP addresses.</i>
dongle	<i>A device that attaches to a computer to control access to a particular application.</i>
encrypt	<i>To scramble information so that only someone who knows the appropriate secret can obtain the original information (through decryption).</i>
end user	<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>
engine	<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>
escrow	<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>
engine	<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>
Federal Information Processing Standard (FIPS)	<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>
group	<i>A named collection of users created for convenience in stating authorization policy.</i>

TERM	DEFINITION
hash	<i>A cryptographic one-way function that takes an arbitrary-sized input and yields a fixed-size output. [1]</i>
immutable	<i>Unchangeable. [2]</i>
integrity	<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>
interface	<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>
international data encryption algorithm (IDEA)	<i>A secret key cryptographic scheme. [1]</i>
international Standards Organization (ISO)	<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>
internet Engineering Task Force (IETF)	<i>A standards body that focuses on protocols for use in the Internet. Its publications are called Internet RFCs (Requests for Comment). [1]</i>
intrusion Detection Systems (IDS)	<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>
key	<i>A quantity used in cryptography to encrypt or decrypt information.</i>
key escrow	<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>
log	<i>To record an action. [2]</i>
log file	<i>A file that lists actions that have occurred. [2]</i>
message authentication code (MAC)	<i>A synonym of message integrity code (MIC). [1]</i>
manager	<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>
message digest	<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>
multifactor	<i>More than two elements or quantities.</i>
message integrity code (MIC)	<i>A fixed-length quantity generated cryptographically and associated with a message to reassure the recipient that the message is genuine. [1]</i>
NIST	<i>National Institute of Standards and Technology</i>
non-repudiation	<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>
network time protocol (NTP)	<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>

TERM	DEFINITION
online certificate status protocol (OCSP)	<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>
offline attack	<i>An attack performed while offline to the system being attacked (see also “dictionary attack”).</i>
one-time passwords	<i>Passwords that can only be used once. [2]</i>
operator	<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>
orthogonal	<i>Having to do with right angles; rectangular. [5]</i>
packet filters	<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>
passive attack	<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>
password	<i>A supposedly secret string used to prove one’s identity. [1]</i>
personal identification number (PIN)	<i>A short sequence of digits used as a password. [1]</i>
public key cryptography standards (PKCS)	<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>
plaintext	<i>Unencrypted data. [3]</i>
port number	<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>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></i>
pre-authentication	<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>
private key	<i>The quantity in public key cryptography that must be kept secret. [1]</i>
privileged user	<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>
product administrator	<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>
protected path	<i>A mechanism that guarantees a mutually authenticated channel. [4]</i>
public key	<i>The quantity in public key cryptography that is safely divulged to as large an extent</i>

TERM	DEFINITION
	<i>as is necessary or convenient. [1]</i>
public key cryptography	<i>A cryptographic system where encryption and decryption are performed using different keys. (See asymmetric key cryptography.) [2]</i>
relying party	<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>
replaying	<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>
repudiation	<i>Denying that one did something or made some statement. [1]</i>
resource	<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>
revoke	<i>To withdraw, repeal, rescind, cancel or annul. [5]</i>
role	<i>A function or office assumed by someone. [5]</i>
security domains	<i>The sets of objects that a subject has the ability to access. [3]</i>
security features	<i>The security-related functions, mechanisms and characteristics of AIS hardware and software. [3]</i>
server	<i>A resource available on the network to provide a service, such as name lookup, file storage or printing. [1]</i>
sign	<i>To use your private key to generate a digital signature as a means of proving you generated, or approve of, a message.</i>
signature	<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>
simple network management protocol (SNMP)	<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>
spoof	<i>To convince someone that you are entity X when you are not, without X’s permission. [1]</i>
strong authentication	<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>
symmetric key cryptography	<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>
system	<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>
system administrator	<i>In the scope of this profile, an individual (user) who has higher privilege at the operating system level.</i>
system recovery	<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>
system restart	<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>
transmission control	<i>The common name for a family of more than 100 data communications protocols</i>

TERM	DEFINITION
protocol/Internet protocol (TCP/IP)	<i>used to organize computers and data communications equipment into computer networks.</i>
token device	<i>A credit card sized device that generates authentication tokens, such as one-time passwords. [2]</i>
two-factor authentication	<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>
weak authentication	<i>Typically, this implies the conventional use of passwords.</i>
user	<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>
user-ID	<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>
X.509	<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