

---

# ***BITS Product Certification Program***



## ***Access Control Systems Products Profile***

### ***Technical Contact Information***

For more information regarding technical content, please contact:

BITS Product Certification Program

bitslab@fsround.org

Tel: (202) 289-4322

Fax: (202) 289-0193

**Originating Author:** Kevin Brown, Senior Consultant, Predictive Systems, Inc., *Global Integrity™* Information Security Services

**Profile Leader Workgroup Chair:** James Ramsey, Vice President, Information Security Division, Wachovia Corporation

---

BITS Product Certification Program Access Control Systems Products Profile Working Group Members  
(Primary contributors/organizations indicated in **bold**.)

<b>Representative</b>	<b>Organization</b>	<b>Representative</b>	<b>Organization</b>
Gwen Boyd	Wachovia Corporation	Farah Moaven	Wells Fargo & Company
<b>Jim Brown</b>	<b>M&amp;I Data/Metavante</b>	Glen Ottoson	M&I Data/Metavante
Wayne Browning	FleetBoston Financial Corporation	<b>Sam Phillips</b>	<b>Bank of America</b>
<b>Landy Dutton</b>	<b>Regions Financial Corp.</b>	Eddie Schwartz	Nationwide
Brian Ekkebus	Northern Trust Corp.	<b>Howard Taylor</b>	<b>J.P. Morgan Chase &amp; Co.</b>
Parker Foley	Wachovia Corporation	<b>Robert Vonderheid</b>	<b>Comerica Inc.</b>
Gene Fredriksen	Raymond James Financial	<b>Richard Yen</b>	<b>J.P. Morgan Chase &amp; Co.</b>
<b>Eric Guerrino</b>	<b>The Bank of New York Company, Inc.</b>	Emory Anderson	US Department of the Navy

### Profile Feedback

Please send any comments (technical or otherwise) to [bitslab@fsround.org](mailto: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.*

### Access Control Systems Security Products Profile – Version Control History

Note: **Bold** in Version/Date column indicates a public release.

Version / Date	Changes
0.90 – 0.92 (Jan – Mar 2000)	◆ DRAFT – Creation of initial draft (Global Integrity internal)
1.00 (Mar 2000)	◆ DRAFT – Initial distribution – BITS/Profile Leader/Global Integrity
1.01 (Apr 2000)	◆ DRAFT – Working copy – Distribution to Financial Industry Profile Working Group
1.02 – 1.04 (Apr/May 2000)	◆ DRAFT – Financial Industry Working Group review and comment
1.05 – 1.08 (May 2000)	◆ DRAFT – Financial industry/technology provider workshops
1.09 (Jul 2000)	◆ DRAFT – Format restructured following financial industry/technology provider workshop to separate features from functions
<b>1.10</b> <b>(Aug 2000)</b>	◆ DRAFT – Initial public release for comment
<b>1.2</b> <b>(Dec 2000)</b>	◆ FORMAL RELEASE – Available for “product testing” <i>(modifications: 2.1.1;4, 2.1.2;3, 2.1.2;8, 2.1.3;8, 2.1.4;2, 2.1.4;7, 2.1.6;6, 3.3;2)</i> <i>(new: 2.1.3;14, 2.1.6;16, 2.1.8;6)</i>
<b>2.0</b> <b>(May 2003)</b>	◆ Mapped to MSC 3.0 and sections 3 and 4 revised by the Technical Team
<b>2.0</b> <b>(January 2004)</b>	◆ FORMAL RELEASE – Available for “product testing”

# Table of Contents

---

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 OVERVIEW .....	1
1.2 MANDATORY AND DESIRED CRITERIA .....	2
1.3 BOUNDARIES AND UNDERLYING PLATFORMS.....	3
1.4 TEST PLANS AND PROFILES .....	3
1.5 COMMON TERMS USED IN THIS PROFILE.....	4
<b>2. CRITERIA FOR THE ADMINISTRATION AND OPERATION OF ACCESS CONTROL SYSTEMS PRODUCTS .....</b>	<b>5</b>
2.1 SECURITY FEATURES.....	5
3.0 PRODUCT FUNCTIONALITY.....	15
4.0 SCALABILITY.....	16
<b>3. REQUIRED FUNCTIONAL CRITERIA FOR ACCESS CONTROL SYSTEMS SECURITY PRODUCTS .....</b>	<b>17</b>
3.1. OVERVIEW .....	17
3.2 REQUIRED FUNCTIONAL CRITERIA .....	17
<b>4. DESIRED FUNCTIONAL CRITERIA FOR ACCESS CONTROL SYSTEMS SECURITY PRODUCTS</b>	<b>19</b>
4.1 OVERVIEW .....	19
4.2 DESIRED FUNCTIONAL CRITERIA.....	19
<b>APPENDIX A: INDUSTRY STANDARDS.....</b>	<b>20</b>
<b>APPENDIX B: BIBLIOGRAPHY .....</b>	<b>21</b>
<b>APPENDIX C: GLOSSARY OF TERMS .....</b>	<b>22</b>

# 1. Introduction

---

## 1.1 Overview

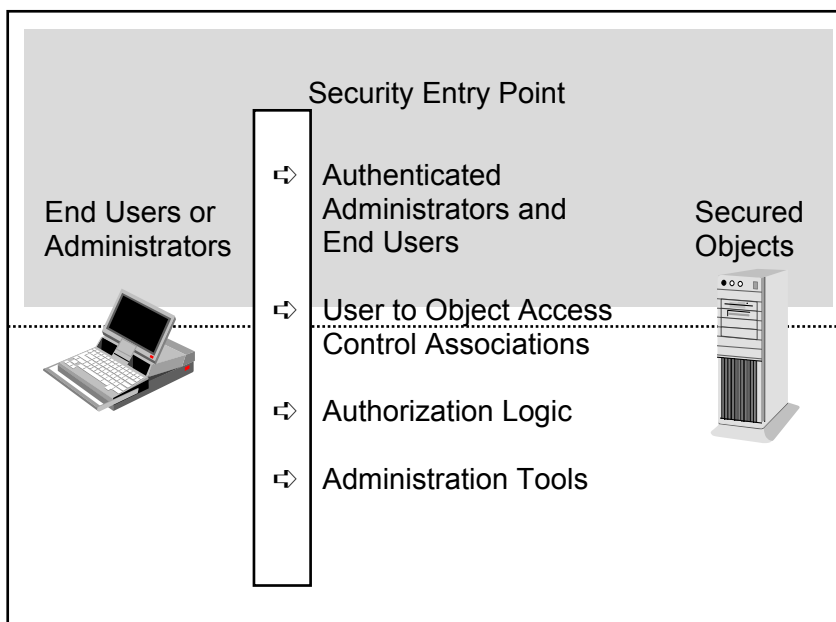
This Product Profile defines the security requirements to support the technical analysis of access control products. This category includes products that authorize user access to system, network, server and application resources, remote access control products, and single sign-on products.

Although access control products are the focal point of this profile, products that provide authorization in support of access control are also addressed here.

This profile lists the security-related criteria that *apply to the features and functionality* normally found in access control products. There is an assumption that a product focused on access control cannot operate securely without the support of other security components (security administration, authentication, etc.) either built into a system or present in the underlying platform or computing environment boundary within which the system is operating.

The criteria have been derived and expanded from the Master Security Criteria (MSC). The MSC defines the basic set of security features, functionality, usability, and scalability requirements that apply to many different product categories. The MSC is a necessary accompanying reference for Section 2.

Tests under this profile will be performed in a standard configuration environment that includes the product and any supporting components. The product profile is composed of criteria that apply to the client and server sides of access control.



*High-level view of a basic access control system and supporting components.*

## 1.2 Mandatory and Desired Criteria

Each criterion will be identified as either *required* or *desired*.<sup>1</sup> A product will earn the *BITS Tested Mark* only if it meets all *mandatory* criteria in Section 2, “Criteria for the Administration and Operation of Access Control Systems Products.” A product will not merit a *BITS Tested Mark* if it misses any one mandatory criterion.

In this document, *mandatory* criteria are indicated with the verb “shall,” while *desired* criteria are indicated with the verb “should.”

Some criteria are identified in the profile document as *desired*. These criteria are not required to obtain the *BITS Tested Mark*, but compliance with them 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.*

---

<sup>1</sup> A criterion is considered *required* unless it is explicitly identified as *desired*.

## 1.3 Boundaries and Underlying Platforms

A number of criteria outlined in this document may be addressed through security features of any system component, rather than the access control systems security product itself. Rather than requiring all security functionality to be provided by the standalone system, the criteria and process allow for 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 these boundaries will include the product itself, as well as 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 product testing (within the agreed-to testing boundary<sup>2</sup> 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 whether the vulnerability is 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: Industry Standards, 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 testing process.

## 1.4 Test Plans and Profiles

Actual testing of individual products will be conducted against a test plan produced from this profile. A specific test plan will be developed for each product undergoing testing. *It is possible that certain criteria will be implemented differently, and thus tested differently, in two similar products.*

Access control systems 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

---

<sup>2</sup> Reference: BITS Lab Testing Services Agreement (and Schedule A, Product Testing Schedule)

system(s). The management console and subordinate systems will each consist of a supporting platform and user interfaces.

## 1.5 Common Terms Used in this Profile

Listed below are definitions of terms that are important or frequently used in the remainder of the profile. See Appendix C: Glossary of Terms for a complete list of terms.

<b>TERM</b>	<b>DEFINITION</b>
<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 may 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 listing actions that have occurred. [2]</i>
<b>Master Security Criteria (MSC)</b>	<i>BITS Product Certification Program criteria used to generate product-specific criteria. The criteria in this document fall into categories outlined in the Security Criteria Overview, and will be used to develop the individual Product Security Profiles. MSC version 3.0 is referenced in 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 in which 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 in order to be able to perform system management functions. [1]</i>
<b>Product administrator</b>	<i>In the scope of this profile, a user with higher privilege at the product’s configuration level (the user may or may not be the same as the system administrator).</i>
<b>System</b>	<i>Within the scope of this profile, the totality of the product and the mediation device(s) (if any) that need to be tested.</i>
<b>System administrator</b>	<i>In the scope of this profile, an individual (user) with higher privileges at the operating-system level.</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 represents the user in data structures, e.g., the owner of a file or process, the person attempting to access a system resource).</i>

## 2. Criteria for the Administration and Operation of Access Control Systems Products

---

### 2.1 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 access control security 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
<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 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
<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 otherwise 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	<i>Authentication of product to product administrator before user gives password.</i>
2.2.1.5	Required	

---

<sup>3</sup> "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.

<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 otherwise identified in the "Comment or Rationale" column.</p>		
2.2.1.6	Required	
2.2.1.7	Required	
2.2.1.8	Required	
<p><b>Subsection 2.2.2: Knowledge and Possession-Based Mechanism Requirements</b></p>		
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	
<p><b>Subsection 2.2.3: Personal Characteristics-Based Mechanism Requirements (DESIRED)</b></p> <p>Note: The classification of "DESIRED" for this subsection indicates the product submitted for evaluation may not need to comply with the criteria in this subsection. However, if the product is claiming to provide the capability, it is <u>not</u> an optional section and the product must fully comply with all criteria in this subsection (2.2.3).</p>		
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
<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 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	<i>In the context of this profile, the term "roles" implies "groups."</i>
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	

---

<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; no user shall be allowed access to a resource (e.g., transaction, data, process, etc.) of the system unless he or she is 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 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
<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	
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	

---

<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.		
2.4.14	Required	

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	

---

<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	<i>Within the context of this profile, the product should have the <u>capability</u> to record all identified events (MSC v3, 2.6.3.1 – 11) as well as to allow the administrator to selectively enable/disable recording of the event.</i>
2.6.4	Required	
2.6.5	Required	
2.6.6	Required	<i>Within the context of this profile, notifications are not limited to email.</i>
2.6.7	Required	<i>Within the context of this profile, notifications are not limited to email.</i>
2.6.8	Required	
2.6.9	Required	
2.6.10	Required	
2.6.11	Required	
2.6.12	Required	

---

<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; 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	

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	
2.8.7	Required	
2.8.8	Required	
2.8.9	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 events such as system restart, disaster recovery, arrival of sensitive dates related to the Y2K issue, etc.; provide the backup 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.		
2.8.10	Required	
2.8.11	Required	
2.8.12	Required	

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	

<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 2.9: 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.		
2.9.9	Required	
2.9.10	Required	

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.		
NEW	<b>DESIRED</b>	<i>NEW CRITERIA<sup>13</sup>: 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	

---

<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.

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

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

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<b>MSC Section 2.11: Non-repudiation<sup>14</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.		
NOTE: The classification “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.

### 3.0 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 affected 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 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

---

<sup>14</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.

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	
3.2	Required	

#### 4.0 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 Access Control Systems Security Products

## 3.1. Overview

This section describes the minimum functionality expected in products of this class and criteria associated with each of these functions.

## 3.2 Required Functional Criteria

<i>CRITERIA</i>	<i>RATIONALE</i>
<p>3.2.1 If the product supports a distributed (manage/agent) model for access control:</p> <ul style="list-style-type: none"> <li>• Privileges on “target platforms”<sup>15</sup> must be accordant with access administration policies maintained in the main/central repository. The system shall provide a facility so that a user’s access and privileges on target platforms are the same as access policies in the central repository.</li> <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 to disable the access on the target platforms.</li> </ul>	<p><i>Need in order to ensure that access administration policies remain synchronized between the management and agent/target platforms.</i></p> <p><i>This notification is needed to ensure that an out-of-sync condition in the access administration policies between the management and agent/target platforms has occurred.</i></p>

<sup>15</sup> “Target platforms” are those platforms under administrative interface to main management consoles via agents.

<b>CRITERIA</b>	<b>RATIONALE</b>
<p>3.2.2 The system shall support the ability to control (i.e., change the password, implement a more restrictive password lifetime) all user-IDs or the ability to disable all user-IDs, including pre-defined vendor-supplied and/or systems defaults.</p>	<p><i>The administrator must be able to use the quality of passwords in an environment or domain.</i></p>
<p>3.2.3 For the initial authenticator creation, the system shall not divulge the authenticator to anyone other than the authorized administrator.</p>	<p><i>This is needed to ensure that only appropriate and necessary personnel have access to the initial authenticator.</i></p>
<p>3.2.4 The system shall have the capability to check the integrity of security data read from a backup file when performing a restore function.</p>	<p><i>To ensure an accurate recovery, the system should have the ability to verify the integrity of the security file loaded during a restore function.</i></p>
<p>3.2.5 Any administrator must be reflected in the audit log as an administrator executing a function as an end user. The log must include the ID of the initiating administrator of the event as well as the ID for which the initiating administrator is conducting the event.</p>	<p><i>This is needed to ensure the system maintains a complete audit trail of all auditable activity.</i></p> <p><i>The term “administrator” includes all account types or groups with the ability to act as an end user.</i></p>
<p>3.2.6 The system must incorporate the ability for the end user to authorize an administrator to act as that end user.</p>	<p><i>This is necessary for the end users to provide accountability on the administrator.</i></p> <p><i>The term “administrator” includes all account types or groups with the ability to act as an end user.</i></p>
<p>3.2.7 The system shall allow the audit log to be written both locally and to a secure remote logging environment.</p>	<p><i>This preserves integrity and provides data for forensic investigations.</i></p>

# 4. Desired Functional Criteria for Access Control Systems Security Products

---

## 4.1 Overview

This section lists the desired criteria for the functional areas that are common to products in this profile.

## 4.2 Desired Functional Criteria

<i>CRITERIA</i>		<i>RATIONALE</i>
4.2.1	<b>DESIRED:</b> The system should support a process to process authentication.	
4.2.2	<b>DESIRED:</b> The system should have the ability to integrate with third-party authentication products.	
4.2.3	<b>DESIRED:</b> The system should have the ability to reject any connection attempt or service that is not able to negotiate to a security state that meets the security policy established by the administrator.	

## Appendix A: Industry Standards

---

For the purposes of these criteria, the terms “public and widely used” and “financial industry standards” shall refer to those standards, algorithms, and protocols listed below as well as other relevant standards approved by the following standards 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 those 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

Sources for definitions are listed at the end of this section.

TERM	DEFINITION
<b>access control</b>	<i>A mechanism for limiting use of some resource to authorized users. [1]</i>
<b>account</b>	<i>In terms of a “user account”, an established relationship between a user and a computer, network or information service.</i>
<b>active attack</b>	<i>An attack, such as manipulation of files or addition of unauthorized files, that results in an unauthorized state change. [3]</i>
<b>administrator</b>	<i>Taken 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 a system administrator and/or product administrator, typically having privileges beyond the scope of an end user. See also “end user”, “user” and “product administrator”.</i>
<b>automated information system (AIS)</b>	<i>Any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware. [3]</i>
<b>application programming interface (API)</b>	<i>Typically provided by a software development toolkit.</i>
<b>applet</b>	<i>Typically, a small program not resident on the local system, which, when downloaded, executes from within another application on that local system. For example, dynamically downloaded Java programs that execute in Internet browsers are considered applets.</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 may 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, smart card seed, etc.</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>This happens when more data is put into a buffer or holding area than the buffer can handle, due to a mismatch in processing rates between producing and consuming processes. A buffer overflow 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 containing 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 over 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 factor entitling one to confidence, credit 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>Typically an “offline attack” or “brute force attack”, the process of “guessing” passwords based on a set of key words or characters until a match is made.</i>
<b>digital signature</b>	<i>A method of verifying identities over a network that is based on public key encryption.</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's 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>end user</b>	<i>Taken in the context of this profile and unless otherwise indicated, the end user of the product. See also “user” and “administrator”.</i>
<b>encrypt</b>	<i>To scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption).</i>
<b>escrow</b>	<i>To hold something in safekeeping. Usually indicates putting something into the custody of a third-party for delivery to a grantee only after the fulfillment of specified conditions [5]</i>
<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>TERM</b>	<b>DEFINITION</b>
<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>malicious code</b>	<i>Mobile code software modules designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing unauthorized disclosure of information, corrupting information, denying service, or stealing resources. (Also called “malicious mobile code”.) [6]</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 and the third party can independently verify the source. [1]</i>
<b>NTP</b>	<i>Network Time Protocol</i>
<b>OCSP</b>	<i>Online Certificate Status Protocol</i>
<b>offline attack</b>	<i>An attack performed while the perpetrator is offline to the system being attacked. (See also “dictionary attack”.)</i>
<b>one-time passwords</b>	<i>Passwords that can only be used one time. [2]</i>
<b>operator</b>	<i>In the context of this profile, an “operator” is one who maintains similar relationships and functions as an administrator, and is given different and/or additional privileges than a typical end user of a system.</i>
<b>orthogonal</b>	<i>Relating to or composed of right angles [5]</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 into applications. [2]</i>
<b>plaintext</b>	<i>Unencrypted data. [3]</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>pre-authentication</b>	<i>A protocol for proving one knows one's password before being 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>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>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 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 in which 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 term is usually used to indicate that the entity performing the reply of messages is mounting a security attack.</i>
<b>repudiation</b>	<i>Denying that one did something or made a certain statement. [1]</i>
<b>revoke</b>	<i>To nullify by withdrawing, recalling, or reversing [5]</i>
<b>role</b>	<i>A position or function.[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-relevant functions, mechanisms, and characteristics of automated information system (AIS) hardware and software. [3]</i>
<b>server</b>	<i>A resource available on a network that provides a particular service such as name lookup, file storage, or printing. [1]</i>
<b>sign</b>	<i>To use one's private key to generate a digital signature as a means of proving one generated, or approve of, some message.</i>
<b>signature</b>	<i>A quantity associated with a message that only someone with knowledge of one's private key could have generated, but which can verified through knowledge of one's public key. [1]</i>
<b>spoof</b>	<i>To convince someone that one is a certain entity X when one is not X, 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>
<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) to be tested. [SCO 2.1.1]</i>
<b>system administrator</b>	<i>In the scope of this profile, an individual (user) having higher privilege at the operating system level.</i>

<b>TERM</b>	<b>DEFINITION</b>
<b>system restart</b>	<i>To restart a system. Also called a “warm boot” when the system is restarted from an operational state. A “cold boot” occurs when the system is powered off and then on again.</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>

**The following sources were used to create this glossary:**

- [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*, NSA, 1998
- [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] *Webster’s II New College Dictionary*, 1999
- [6] Department of Defense Memorandum on Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems, Department of Defense, November 7, 2000