
Financial Services Security Laboratory



Authentication Systems Profile

Technical Contact Information

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

Financial Services Security Lab
c/o Global Integrity Corporation
(888) 660-0134 or +1.703.375.2100
bitslab@globalintegrity.com
BITS
+1.202.289.4322

Originating Author: Rajaram Pejaver, Senior Security Consultant, Global Integrity Corporation

Profile Leader: Parker Foley, First Union Corporation

Profile Feedback

If you have comments regarding this profile, please send an email to <mailto:bitslab@globalintegrity.com>. Include the profile name, your name, e-mail address, telephone, and FAX number, and whether you would like to be contacted. *Please note ... BITS and Global Integrity will take all comments under advisement, but reserves the right to include or exclude comments received in the final criteria.*

Authentication Systems Profile – Version Control History

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

Version / Date	Changes
0.90 – 0.92 (Jan – Feb 2000)	◆ DRAFT - Originating Document Produced
1.00 - 1.10 (Feb - Mar 2000)	◆ DRAFT - Initial Distribution – BITS/Profile Leader/Global Integrity/Work Group
1.11 (April 2000)	◆ DRAFT - Public Comment Version
1.11a – 1.12b (Mar – Aug 2000)	◆ DRAFT - Financial Industry / Technology Provider Workgroup review(s)
1.2 (Aug 2000)	◆ Formal Release of Product Profile for Product Testing

Table of Contents

1. INTRODUCTION	1
OVERVIEW.....	1
BACKGROUND	2
MANDATORY AND DESIRED CRITERIA	4
MULTIFACTOR AUTHENTICATION	5
BOUNDARIES AND UNDERLYING PLATFORMS	5
TEST PLANS AND PROFILES	6
TERMS USED IN THIS PROFILE.....	6
2. GENERAL CRITERIA FOR AUTHENTICATION SYSTEMS.....	7
2.1 USER REGISTRATION AND DELETION	9
2.1.1 <i>Identification</i>	9
2.1.2 <i>Authentication</i>	9
2.1.3 <i>Access Control</i>	9
2.1.4 <i>Integrity</i>	11
2.1.5 <i>Confidentiality</i>	11
2.1.6 <i>Audit</i>	11
2.2 USER LOGIN AND LOGOUT (AUTHENTICATION & DISCONNECT).....	11
2.2.1 <i>Identification</i>	11
2.2.2 <i>Authentication</i>	11
2.2.3 <i>Access Control</i>	12
2.2.4 <i>Integrity</i>	12
2.2.5 <i>Confidentiality</i>	12
2.2.6 <i>Audit</i>	13
2.3 STORAGE OF CREDENTIALS AT CLIENT SITE.....	13
2.3.1 <i>Identification</i>	13
2.3.2 <i>Authentication</i>	13
2.3.3 <i>Access Control</i>	14
2.3.4 <i>Integrity</i>	14
2.3.5 <i>Confidentiality</i>	14
2.3.6 <i>Audit</i>	14
2.4 STORAGE OF INFORMATION BY THE AUTHENTICATION SERVER.....	14
2.4.1 <i>Identification</i>	14
2.4.2 <i>Authentication</i>	15
2.4.3 <i>Authorization</i>	15
2.4.4 <i>Integrity</i>	15
2.4.5 <i>Confidentiality</i>	16
2.4.6 <i>Audit</i>	16
2.5 KEY AND PASSWORD MANAGEMENT.....	17
2.5.1 <i>Identification</i>	17
2.5.2 <i>Authentication</i>	17
2.5.3 <i>Access Control</i>	18
2.5.4 <i>Integrity</i>	18
2.5.5 <i>Confidentiality</i>	18
2.5.6 <i>Audit</i>	18
2.6 AUTHENTICATION PROCESS.....	19
2.6.1 <i>Identification</i>	19
2.6.2 <i>Authentication</i>	19
2.6.3 <i>Access Control</i>	19
2.6.4 <i>Integrity</i>	20
2.6.5 <i>Confidentiality</i>	21
2.6.6 <i>Audit</i>	21
2.7 INTEGRATION AND USABILITY.....	22
2.7.1 <i>Identification</i>	23
2.7.2 <i>Authentication</i>	23

2.7.3 Access Control..... 23

2.7.4 Integrity..... 23

2.7.5 Confidentiality..... 24

2.7.6 Audit..... 24

3. CRITERIA FOR PASSIVE AUTHENTICATION SYSTEMS..... 25

3.1. INTRODUCTION..... 25

3.2. CRITERIA..... 25

4. CRITERIA FOR TRUSTED THIRD PARTY SYSTEMS..... 28

4.1. INTRODUCTION..... 28

4.2. CRITERIA..... 28

5. CRITERIA FOR TOKEN BASED SYSTEMS 30

5.1. INTRODUCTION..... 30

5.2. CRITERIA..... 30

6. CRITERIA FOR PUBLIC KEY SYSTEMS..... 32

6.1. INTRODUCTION..... 32

6.2. CRITERIA..... 32

7. CRITERIA FOR BIOMETRICS SYSTEMS 34

7.1. INTRODUCTION..... 34

7.2. CRITERIA..... 34

APPENDIX A: INDUSTRY STANDARDS 35

APPENDIX B: MSC CROSS-REFERENCE MATRIX..... 37

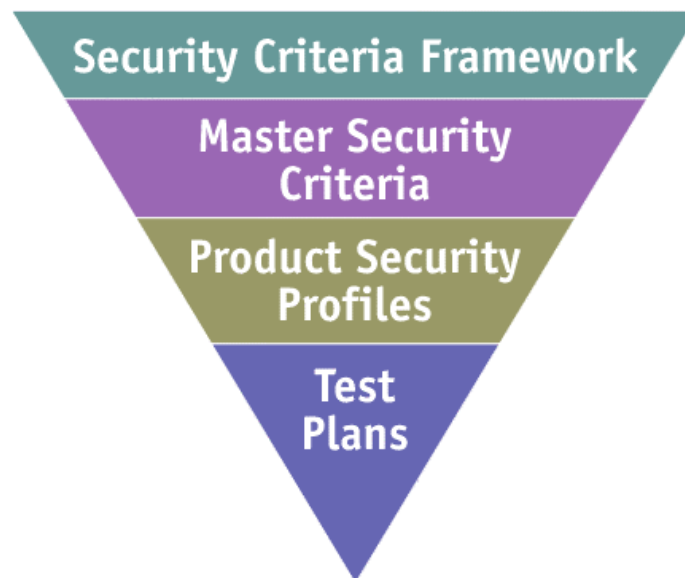
APPENDIX C: BIBLIOGRAPHY 52

APPENDIX D: GLOSSARY OF TERMS..... 53

1. Introduction

Overview

This Product Profile defines the security requirements to support the technical analysis of Authentication products. These software and hardware products help verify the authenticity of users and application objects. The profile lists the security-related criteria that apply to authentication systems and to the features and functions normally found in authentication systems. The criteria have been derived and expanded from the Master Security Criteria¹. The Master Security Criteria define the basic set of security features, functionality, usability and scalability requirements that apply to many different product categories. Note that there may be some requirements in this document that may not be reflected as requirements in the Master Security Criteria. When applicable, after each requirement, there will be a link to the related section and specific requirements in the Master Security Criteria. [MSC, Section; Requirement]



¹ BITS Security Lab Product Profile documents can be found at: <http://www.globalintegrity.com/bitslab>

Background

Authentication is important in computer systems as a basis for Access Control and for Accountability. In general, the “strength” of the authentication system should be proportional to value of assets or data being protected. It is usually not possible to know the value of the asset at the time of the testing of an authentication product. Therefore, this document assumes the asset being protected is of the highest value and lists an extensive set of applicable criteria.

Authentication systems can be used in two distinct situations: (a) to authenticate a human user to a computer system, and (b) to authenticate a non-human entity (like a server process, or a hardware device) to another such entity. The system should distinguish between these two situations because, depending on the situation, some of the criteria are markedly different.

There is a variety of authentication technologies. A single set of criteria will not apply to all the technologies. In other words, a criterion that is essential to one technology may be totally meaningless to a different technology. Hence, this profile is divided into two parts: the first part lists criteria that are common to all technologies, and the second part lists criteria that are specific to different classes of available technologies.

To list the classes of technologies, we note that traditionally, there have been three orthogonal forms of authentication:

1. Something the user knows,
2. Something the user has or possesses,
3. Some immutable characteristic of the user.

This product profile further divides the above classes into six major categories. They are listed (as items “a” through “g”) below, along with examples of technologies that fit into each category.

Something the user knows

- a. Passive Authentication based systems
 - ◆ native OS password based systems, shadow passwords, add-on enhancement packages, etc.

- ◆ distributed authentication systems, e.g. TACACS, RADIUS, ...
- b. Trusted third party systems
 - ◆ Kerberos based systems
- c. Shared dynamic information
 - ◆ last transaction, security codes provided in the last email or balance statement

Something the user has or possesses²,

- d. Token based systems, or dynamic password systems
 - ◆ magnetic stripe cards, proximity devices, “dongles”, etc.
 - ◆ challenge/response devices, one time password generators, etc.
 - ◆ time based token cards, sequential code generators, ...
- e. Shared Secret based systems³
 - ◆ Symmetric Key systems, one time pads, ...
- f. Public Key based systems
 - ◆ Software based X.509 certificates
 - ◆ Memory token devices that store the private key
 - ◆ Microprocessor based devices, PCMCIA cards, hardware storage modules

Some immutable characteristic of the user.

- g. Biometrics systems.
 - ◆ fingerprints, retinal scans, palm geometry, face recognition,
 - ◆ voice prints, typing patterns, etc.

² Includes systems using a Personal Computer (PC) or some portable device such as a card or hand-held device

³ Passive Authentication systems are not included in the section of Shared Secret based systems

The category specific criteria for the six categories of authentication technologies (listed as “a” through “g” above) are listed in sections 3 through 7 of this document.

There are no category specific criteria for Shared Secret based systems. The criteria for these systems are covered in the section listing the general criteria. Shared Secret systems are those in which a common symmetric key is known to two communicating parties. Since the key is known to only two parties, it can be used to authenticate one party to another. Note that each pair of parties needs to have a unique shared secret key. This type of authentication system is typically used in situations where a fixed set of parties communicate with each other over extended periods of time. Examples of these systems are ATM networks, link encryptors, network routing components, etc.

Mandatory and Desired Criteria

Each criterion will be tagged as being Mandatory⁴ or Desired. A product will get the BITS Tested Mark only if it meets all the mandatory criteria. 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’.

Each desired criterion will have a “Desirability” rating or value. Products that meet these criteria will receive a score in that category depending on the number of desired criteria they meet. The product’s score in each category will be the sum of the ratings of the desired criteria that it meets. The goal of this form of organization of the product profile is to allow potential customers to be able to easily gauge the conformance and effectiveness of tested products.

“Desired” criterion is recognized by the Financial Services industry as advantageous and may become a requirement in the future.

⁴ For better readability, the Mandatory tag is omitted. A criterion must be considered as *Mandatory* unless it is explicitly tagged as being *Desired*.

Multifactor Authentication

A system is referred to as having Multifactor authentication when it uses combinations of the above mechanisms. When designed correctly, multifactor systems can be stronger than systems that rely on a single technology. Typically, two independent technologies, such as Token cards and Biometric technologies, are combined with one of the other technologies to form a multifactor system. These systems should meet mandatory criteria required for each of their specific technologies. It is expected that multifactor systems will have higher product scores because they meet a larger number of desired criteria.

Some systems intrinsically have multifactor properties. For example, some Token devices implement public key operations. They securely store private key data. These devices need to be “unlocked” before they can be used. The user has to unlock the device by submitting some authentication information to the device. In effect, the user has to authenticate themselves to the device, and then use the device to authenticate themselves to the system. In such devices, the first authentication would use password (or biometric) technologies, and the second authentication would use public key technologies. For the device to merit the BITS Tested Mark, the first authentication should comply with the mandatory criteria for passwords (or biometrics) and the second authentication should comply with the criteria for public key systems. Note that in such situations, authentication is serial and the strength of the overall system is only as strong as the weakest link in the chain.

Boundaries and Underlying Platforms

A number of criteria outlined herein may be addressed through security features of any component, rather than authentication systems 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., operating system) or supporting components for security. To support this, the process allows the Technology Provider to define the “boundaries” of the test environment, which delineates the system to be tested. It is anticipated that this boundary will include the product itself, the underlying platform, and any relying application or system. It is

important to note, however, that the criteria will be applied equally to all components within that boundary.

Test Plans and Profiles

It is important to note that actual testing of individual products will be conducted against a test plan produced from this profile. A specific test plan will be developed by the Security Lab in conjunction with the Technology Provider, for each product undergoing testing. *It is entirely possible that certain criteria will be implemented differently, and thus tested differently, in two similar products.*

Systems will be tested within a standard configuration and standalone environment⁵ that will include an access control & administration system product and the supporting platform and user interfaces.

Terms Used in this Profile

Please reference this profile's "Appendix D: Glossary of Terms" for details.

⁵ Reference "Boundaries and Underlying Platforms" section of this document for clarification of tested components

2. General Criteria for Authentication Systems

This section lists the criteria that are common to most authentication systems. The criteria are grouped according to the functionality provided by a typical Authentication product. This results in the following seven groups listed below. Examples of the functionality are also listed for each group.

User Registration and Deletion

- a. Who can add & remove users
- b. Validation of users before adding
- c. Ensure unique User-IDs
- d. Suspending & restoring users

User login and logout (Authentication & Disconnect)

- a. If user login and logout services are provided, protecting display of password entered
- b. Restricting the number of login attempts
- c. If the system provides login and logout services, restricting duration of inactive session

Storage of credentials at client site

- a. Encryption of the secret information
- b. Authorized recovery issues
- c. Portability

Storage of information by Authentication Server

- a. Protection of user and authentication server secret information
- b. Access control of this information
- c. Backup/Recovery
- d. Integrity of stored Public Key certificates

- e. Confidentiality of private keys used for encryption
- f. Storage and integrity of Audit log

Key and password management

- a. Generation of all cryptographic materials
- b. Generation of random passwords
- c. Password reset
- d. Use of authentication key for encryption of data not involved in the authentication process, such as session data.
- e. Changing passwords and keys
- f. Testing passwords and keys

Authentication process

- a. Integrity of the protocol and algorithm against attacks from design viewpoint.
- b. Integrity of the protocol and algorithm against attacks from implementation viewpoint.
- c. Scalability & Performance issues
- d. Vulnerability of system to various attacks, including: buffer overflow attacks, denial of service attacks, etc.

Integration and Usability

- a. Integration with user management applications, HR systems, etc.
- b. Integration with other authentication and single sign on (SSO) systems.
- c. Integration with report generators

Within each of the functional sections above, we will examine the impact of the typical six security functions (Identification, Authenticity, Confidentiality, Integrity, Authorization, and Audit). This will result in criteria that can then be referenced back to the MSC.

Additional criteria that are unique to a specific authentication technology are listed in the sections following this one.

2.1 User Registration and Deletion

This functional group deals with the administrative capability to add and delete user accounts. It also covers the capability to suspend active user accounts and later restore them.

2.1.1 Identification

1. The system shall unambiguously identify each user with the help of a unique identifier such as a user-ID. [MSC, 2.1.1; 1]
2. The system shall support separate user-IDs for every Administrator and Operator of the system. [MSC, 2.1.1; 1]

2.1.2 Authentication

3. The system shall support multifactor authentication for the authentication of administrators. [NEW]
4. **DESIRED**: The system should allow for the identity of each user to be independently verified before a new user-ID is issued. [NEW]

2.1.3 Access Control

5. The system shall allow only authorized administrators to create or delete user-IDs. [NEW]
6. The system shall have the capability to activate a previously created credential. [NEW]
7. The system shall support separate sets of privileges for staff who install and maintain the system (e.g. system administrators) and for staff who operate the system by following an operational security policy (e.g. system operators). [MSC, 2.1.3; 11]

8. The system shall have the capability to enforce the immediate revocation of a user and the associated keying material when requested by the administrator. [MSC, 2.1.4; 11]
9. The system shall have the capability to automatically disable⁶ an identifier if it remains inactive for an administrator specifiable time period (e.g., three months). [MSC, 2.1.1; 5]
10. **DESIRED**: User-IDs related to human users should be configurable (i.e. individually, by groups or all User-IDs) so that they expire after an administrator specifiable period (for example, 6 months.) User-IDs associated with non-human objects (e.g., production batch jobs, servers, routers, etc.) may be excluded from this requirement. [NEW]
11. **DESIRED**: User-IDs that expire should be renewable via a secure re-enrollment procedure⁷. [NEW]
12. **DESIRED**: The system should maintain all or some of the following security attributes for each user account: user-ID, group memberships, authentication information and security-relevant roles. These attributes shall be associated with the account. Any security related attributes that are maintained shall be stored securely so that their confidentiality and integrity are protected. [MSC, 2.1.1; 6]
13. **DESIRED**: The system should allow only administrators to suspend and restore User-IDs. [NEW]
14. **DESIRED**: The system should allow delegation of administrative authority so that specific administrative accounts may have authority over subsets of user accounts. Further, it should be possible to delegate only subsets of authority to some administrator accounts. [NEW]

⁶ The disabling process need not be automatic. For example, the system may generate an autonomous message for the administrator indicating that a user-ID has remained inactive for the specified period. It is expected that the administrator will disable the user-ID. However, an automatic disabling feature shall exist that the administrator may enable.

⁷ A secure enrollment process must take steps to ensure the confidentiality and authenticity of a user-ID re-enrollment. At a minimum, it must enforce the same principles of assurance followed during the original user enrollment.

2.1.4 Integrity

15. The system shall not allow an administrator to create, intentionally or inadvertently, a user-ID that already exists. [MSC, 2.1.1; 3]
16. The system shall not permit a user-ID to exist without authentication information. [NEW]
17. **DESIRED**: The system should not allow an administrator to create a user-ID that was recently deleted, unless the administrator explicitly overrides the system. [NEW]

2.1.5 Confidentiality

18. The system shall not reveal the passwords or privileges of a new account to unauthorized staff or users. [NEW]

2.1.6 Audit

19. The system shall create an audit record for each user creation, deletion, suspension and restoration event. [MSC, 2.1.6; 4]

2.2 User login and logout (Authentication & Disconnect)

This functional group deals with users (and other non-human subjects) authenticating themselves to the system. It also deals with logging out of the system at the end of the connection.

2.2.1 Identification

20. The system shall require a user-ID to be presented for authentication. Anonymous IDs shall not be authenticated. [NEW]

2.2.2 Authentication

21. The system shall not impede the re-authentication of users if so required by the relying parties. [NEW]

2.2.3 Access Control

22. The system shall limit the number of failed login attempts. This protects against online dictionary attacks. If several consecutive incorrect login attempts are made, the system shall generate an alarm after an administrator-specified number of attempts. The maximum allowed is four attempts. [MSC, 2.1.3; 3]
23. When an administrator-specified threshold for invalid consecutive attempts is reached, the system shall be configurable to deactivate access for the user ID until an administrator unlocks it. [MSC, 2.1.3; 4]
24. **DESIRED**: The system should provide a capability to enforce a session inactivity “time-out” feature for administrator / operator accounts accessing the system itself, as required by the local policy, the application or the relying parties. If there is no activity on a session associated with human users for an administrator-specified period, the system shall lock out the session and require a re-authentication to restore access. Unattended sessions between processes and services should be excluded. [MSC, 2.1.3; 7]
25. **DESIRED**: At the time of login to the authentication system itself, the system should provide the capability to generate an authorized administrator configurable warning banner. The administrator should have the capability to create a warning banner that conforms to corporate policy and complies with appropriate state and local laws. [MSC, 2.1.3; 5]

2.2.4 Integrity

26. If a session is interrupted by a disruption due to power failure, system crash, transmission problems, or is terminated by the user, the connection shall be terminated. The establishment of a new session will require the normal user identification, authentication and authorization. [MSC, 2.1.3; 8]

2.2.5 Confidentiality

27. The password entered by the administrator shall not be displayed while it is being typed in. [NEW]

28. During a login, the system shall allow the entire login sequence to be completed before providing any response. [MSC, 2.1.3; 2]
29. Error feedback during the authentication procedure⁸ shall provide no information to the user⁹ other than “invalid” (i. e., it shall not reveal which part of the authentication procedure is incorrect). [MSC, 2.1.2.1; 3]

2.2.6 Audit

30. The system shall have the capability to create an audit record for each authentication success, authentication failure and lockout event. [MSC, 2.1.6; 4]

2.3 Storage of credentials at client site

Most authentication systems maintain state in the form of user credentials at the user’s workstation for the duration of the user’s logged in session. This data must be stored securely to prevent it from being copied or modified in an unauthorized manner. This section also covers situations where a server or an application has to initialise itself and run without any operator intervention.

2.3.1 Identification

[None]

2.3.2 Authentication

31. If the user’s private or secret authentication information is stored at the client site, then the users shall have to authenticate themselves before they are allowed to access the information. For example, user authentication shall be required before the users are allowed to access their private key. [NEW]

⁸ Authentication Procedure indicates the authentication process to the system itself

⁹ Within the content of this criteria, “user” indicates “administrator” (or equivalent)

32. Unattended server processes shall be able to use operating system provided authentication to access the security-related information that they require for their operation. [NEW]

2.3.3 Access Control

33. User credentials and other sensitive data stored on workstations shall be protected against unauthorized viewing. [NEW]

2.3.4 Integrity

34. User credentials and other sensitive data stored on workstations shall be protected against unauthorized tampering. [NEW]

2.3.5 Confidentiality

35. If keying material is generated and stored, the system shall provide secure key storage that is impractical¹⁰ to compromise through a logical or physical attack. [MSC, 2.1.4; 4]

2.3.6 Audit

[None]

2.4 Storage of information by the Authentication Server

This functional group deals with the security of sensitive data stored by the Authentication Server at locations away from the user's workstations. This includes the Directory & LDAP server, various databases, file systems, backup tapes, etc.

2.4.1 Identification

36. If the authentication system uses a database or file system to store information, then the authentication system shall use a unique User-ID to access the database or file system. [NEW]

¹⁰ An attack can be considered impractical if the cost of the attack exceeds the value of the potential benefits gained by a successful breach.

2.4.2 Authentication

37. If the authentication system uses a database or file system to store information, then access to that data shall require authentication. [NEW]

2.4.3 Authorization

38. The audit log shall be protected from unauthorized access, modification or deletion. [MSC, 2.1.6; 6]
39. If the authentication system uses a database or file system to store information, then access to that information shall be restricted to the authentication system. [NEW]

2.4.4 Integrity

40. If the authentication system uses a database or file system to store information, then the integrity of that data shall be preserved. It shall not be possible to bypass the authentication system and modify the data. [NEW]
41. During system restart, authentication information shall be recoverable without loss of data and system integrity. [NEW]
42. The system shall have the capability to be recovered back to a known earlier state. This operation shall require proper authorization. [NEW]
43. The system shall have the capability to protect data integrity by performing data integrity checks such as [MSC, 2.1.5; 10]:
 - ⇒ Proper rule checking on data updates;
 - ⇒ Verification of message authentication code (MAC), keyed Hash Message Authentication Code (HMAC) or digital signature;
 - ⇒ Adequate alert messages in response to potentially damaging commands before execution;
 - ⇒ Proper handling of duplicate and multiple inputs;
 - ⇒ Proper handling of securely generated encryption keying information;

⇒ Proper handling of overflow conditions.

44. The system shall have the capability to protect the integrity of audit log records by generating integrity checks (e.g., checksums) when the log records are created. [MSC, 2.1.5; 8]

2.4.5 Confidentiality

45. The system shall protect the authentication information database from unauthorized use. [NEW]
46. During system recovery, authentication information shall be recoverable without unauthorized disclosure. [MSC, 2.1.2.1; 6]
47. Only the public and widely accepted or financial services industry standard encryption algorithms listed in Appendix A shall be supported by the system. [MSC, 2.1.4; 6]
48. The system shall not store security-related information¹¹ in the clear. [MSC, 2.1.4; 2]
49. Systems shall support multiple standard algorithms and key lengths to ensure appropriate levels of security. The administrator shall be able to configure the default algorithm and key length. Standard cryptographic algorithms are listed in Appendix A. [MSC, 2.1.4; 7]

2.4.6 Audit

50. The system shall maintain an audit log (e.g., a history file) that provides adequate information for establishing audit trails on security breaches (as part of post-mortem analysis) and user activity. [MSC, 2.1.6; 1]
51. As a minimum, the audit log shall record events as specified in the MSC. [MSC, 2.1.6; 4]
52. For each recorded event mentioned above, the audit log, at a minimum, shall record information as specified in the MSC. [MSC, 2.1.6; 5]

¹¹ "security information" is any information that enforces the security policy of the system

53. The audit log shall maintain the confidentiality of the authenticators (e.g., passwords) by excluding them from being recorded. [MSC, 2.1.6; 3]
54. The system shall prevent unauthorized disabling of the audit function. Any disabling will be noted in the audit log. [MSC, 2.1.6; 12]
55. **DESIRED**: If the system is running with the audit log disabled, then there should be a clear and continuous indicator to alert and remind the operator. [NEW]
56. **DESIRED**: Upon successful session establishment, the system should have the ability to provide the date and time of the last successful login. [MSC, 2.1.3; 6]
57. **DESIRED**: The system should generate a real-time alarm for the impending failure (e.g., running out of storage space) of the audit feature. [MSC, 2.1.6; 8]
58. **DESIRED**: The system should provide an administrator with audit analysis tools to selectively retrieve records from the audit log to perform functions such as producing reports, establishing audit trails, etc. [MSC, 2.1.6; 10]

2.5 Key and Password Management

This section deals with the generation, use and disposal of all cryptographic material.

2.5.1 Identification

[None]

2.5.2 Authentication

59. If the system allows administrators to set user's passwords for new or reinstated accounts, it shall require that users change these passwords when the account is next used before further system access is allowed. [NEW]

2.5.3 Access Control

60. The system shall have the capability to enforce, in real time¹², the revocation of a user and the associated keying material as and when requested by the administrator. [MSC, 2.1.4; 11]
61. The system shall support dual custody of all encryption keys for the purpose of recovery of encrypted data. [MSC, 2.1.4; 12]

2.5.4 Integrity

62. An Authentication Key shall not be used for data encryption purposes. [NEW]
63. **DESIRED**: The system should have the capability to enforce the administrator-specified time period for the validity of keying material for a particular use and/or user. [MSC, 2.1.4; 9]

2.5.5 Confidentiality

64. Once the administrator-specified time period for valid use of keying material has expired, the system shall prevent further use of the keying material. If the system has to support keying material recovery, then the system has to provide for the authenticated and authorized access to the pertinent keying material. [MSC, 2.1.4; 10]
65. If keying material is generated and stored, the system shall provide secure key storage that is impractical¹³ to compromise through a logical or physical attack. [MSC, 2.1.4; 4]

2.5.6 Audit

[None]

¹² The time required for the revocation to take effect will vary depending on the function. The exact time will be specified in the Test Plan for a specific product and may depend on the claim made by the vendor.

¹³ An attack can be considered impractical if the cost of the attack exceeds the value of the potential benefits gained by a successful breach.

2.6 Authentication Process

This section deals with the protocols, design and architecture of the authentication server process.

2.6.1 Identification

66. The system shall have a mechanism such that the execution of security administration functions can be reserved only for an appropriate administrator role (i.e., all other users shall be denied this permission). [MSC, 2.1.9; 1]
67. **DESIRED**: The system should have the capability to identify the originator of any information received from a network interface by IP address, port number, etc. [MSC, 2.1.5; 2]

2.6.2 Authentication

68. The system shall not allow any user to bypass the authentication process. [MSC, 2.1.2.1; 8]
69. **DESIRED**: The system should provide a protected path between it and the objects being authenticated so that the communications cannot be compromised. [NEW]
70. **DESIRED**: The system should have the ability to authenticate itself to the user and to other software application components during the authentication sequence. [MSC, 2.1.2.1; 4]

2.6.3 Access Control

71. The system shall not allow access to the authentication system resources without checking the assigned rights and privileges of the authenticated user. The system shall not allow access to any resource without invoking the authorization process. [MSC, 2.1.3; 1]
72. The system shall not allow a less privileged user to spoof as a highly privileged user. [MSC, 2.1.3; 22]
73. **DESIRED**: The system should provide an enforceable mechanism through which users can be segmented into roles (e.g., administrator),

involving access to security functions and other administrative functions.
[MSC, 2.1.3; 11]

74. **DESIRED**: The system should provide information to the administrator, the application, or the relying party regarding the number of concurrent logon sessions for a given user. [MSC, 2.1.3; 20]

2.6.4 Integrity

75. The authentication process shall prevent replay attacks by protecting the authentication information during network transmission thereby preventing an attacker from examining the sequences of authentication information.
[MSC, 2.1.2.1; 2]
76. The system shall be implemented with proper boundary checking so that buffer overflow conditions are not possible. [MSC, 2.1.8; 2]
77. The encryption algorithms used by the authentication protocol shall be one of the approved algorithms (see Appendix A) and should be widely accepted as being secure. [MSC, 2.1.4; 6]
78. If the system uses a random number generator, then the algorithm used shall be verified to be secure¹⁴. [NEW]
79. The system shall have the capability to protect its integrity by performing data integrity checks such as: Rule checking on data updates; Input validation, Verification of message authentication code (MAC) on data structures; Generation of alert messages in response to potentially damaging commands before execution; etc. [MSC, 2.1.5; 10]
80. The system shall not allow any user to bypass the administrator-configured data integrity controls. [MSC, 2.1.5; 9]
81. The system shall be able to continue to operate securely when various operating parameters increase or decrease. These operating parameters include number of users, active sessions, requests for security function

¹⁴ The Technology Provider will provide the Security Lab detailed information on the random number generator, which supports their claim for randomness and security.

support, generation and distribution of keying material, access control checks, and transactions. [MSC, 2.4; 1]

82. The system shall provide an administrator with the capability to perform secure recovery. The system shall provide an administrator with the capability to back-up and restore all security-relevant data, such as system configurations, user profiles, and access permissions. The system shall have the capability to check the integrity of security data read from a back-up file when performing a restore function. [MSC, 2.1.8; 5]
83. The system shall retain the existing security parameters after a restart. [MSC, 2.1.8; 6]
84. The system shall provide mechanisms to detect, in real-time, replay attacks that duplicate an authentic message. [MSC, 2.1.5; 4]
85. **DESIRED**: The system should have the capability to securely record information related to the reception of specific information from a user (administrator) or another system. [MSC, 2.1.11; 1]
86. **DESIRED**: The system should have the capability to securely link received information with the originator of the information and other characteristics such as time and date. [MSC, 2.1.11; 2]
87. **DESIRED**: The system should provide an administrator with the capability to perform integrity checks (e.g., synchronization points, checksums) on system data and software. [MSC, 2.1.8; 4]

2.6.5 Confidentiality

88. The system shall securely recover all of the security settings and stored security parameters during the normal recovery operation. [MSC, 2.3; 7]
89. **DESIRED**: The system should restrict the capability to overwrite memory and storage to an authorized user. [MSC, 2.1.7; 2]

2.6.6 Audit

90. The system shall provide access to authorized individuals to enable the retrieval, copying, printing, deletion and upload of an audit log. [MSC, 2.1.9; 7]

91. If the audit log malfunctions, the system shall have the capability to generate a real-time alarm. [MSC, 2.1.6; 7]
92. The audit log and its control mechanisms shall maintain integrity and completeness through system restarts. [MSC, 2.1.6; 11]
93. **DESIRED**: The system should provide an administrator with the capability to monitor the state of availability of critical system resources (e.g., overflow indication, lost messages, and buffer queues). [MSC, 2.1.8; 1]
94. For software and data created or modified in the authentication system, the system shall provide an administrator with the capability to retrieve the user-ID, date and time associated with that creation or modification. [MSC, 2.1.8; 3]
95. **DESIRED**: The system should provide an administrator the capability to independently and selectively monitor (in real-time) the actions of any user currently logged on and lock out that user if necessary. [MSC, 2.1.9; 3]
96. **DESIRED**: The system should have the capability to restrict session establishment based on time-of-day, day-of-week, calendar date of the login, and source of the connection (such as IP address and port). [MSC, 2.1.3; 9]

2.7 Integration and Usability

This section deals with the way the authentication system integrates with the surrounding components. Specifically, integration deals with three kinds of systems:

- ◆ systems that feed into the authentication system, like HR and user management systems,
- ◆ other authentication, authorization or single sign-on systems that are installed,
- ◆ systems that get input from the authentication system, such as report generators.

- ◆ Applications or application systems that rely on the authentication system for authentication services by using an API.

2.7.1 Identification

97. The system shall provide a clear and consistent interface (e.g., menu-driven) to facilitate the user and security administration roles. [MSC, 2.3; 2]
98. The system shall enable an administrator to configure individual users or groups of users with specific security characteristics. [MSC, 2.3; 6]

2.7.2 Authentication

99. **DESIRED**: The system should provide information regarding the identity of the authenticated party to the application or relying party. [NEW]
100. **DESIRED**: The system should provide information to the application or relying party regarding the strength of the mechanism used to authenticate a user-ID. [NEW]

2.7.3 Access Control

101. The system shall provide the capability for the administrator role to be able to override vendor-provided security defaults. [MSC, 2.1.9; 8]
102. The system shall provide an administrator, for the purposes of administration sessions, the capability to specify all security parameters, such as individual user-IDs and passwords, password aging intervals, time-out intervals, various alarm conditions, access permissions, and text of the warning banner¹⁵. [MSC, 2.1.9; 6]

2.7.4 Integrity

103. The system shall have the capability to preserve the integrity of its software and data remotely loaded into the system. [MSC, 2.1.5; 7]

¹⁵ The implication is that security parameters should not be hard-coded. Instead, they should be settable by the administrator by executing appropriate commands.

104. The security functionality provided by the system shall be resistant to attacks on external infrastructure components the authentication system itself requires, such as DNS, NTP, etc. [NEW]
105. The system shall provide the security functions in a consistent manner. For example, the terminology used in various administration screens should be consistent. The behavior of similar or related functions should be consistent. [MSC, 2.2; 4]
106. The system shall provide adequate alert messages (e.g., "Do you really mean it?") in response to potentially damaging commands before execution. [MSC, 2.1.8; 7]
107. The system shall conform to the guidance specifications defined in the MSC. [MSC, 2.1.10; 1]
108. The user feedback (for administrators) shall be adequate and timely (e.g., real-time) to prevent the user from entering incorrect data (e.g., typographical errors). [MSC, 2.3; 4]

2.7.5 Confidentiality

[None]

2.7.6 Audit

109. **DESIRED**: An administrator should have the capability to generate a status report detailing the values of the parameters and flags that affect secure operation of the system. [MSC, 2.1.8; 8]

3. Criteria for Passive Authentication Systems

3.1. Introduction

Passive authentication refers to a large class of simple systems that use password verification. The authentication for these systems are typically classified as being “weak”, in that the user has to present a password to the system. Typically, for this class of systems, there is no special authenticating hardware involved, and verification consists of a simple table lookup.

These systems typically use passwords, or pass-phrases, or PINs. Products in this space attempt to enhance the password verification functionality provided by the base operating system or application. Examples of these products are Shadow Passwords, Passwd+ (enhances passwords for Unix), DLLs for NT authentication, etc.

This class of systems include Server based authentication systems, where the authentication software is distributed on multiple hosts. A separate process, which is typically on a centralized server on the network, holds the user’s secret authentication information in an encrypted form. The user will present the password to a client component, which then communicates with the server to verify the password. The advantage of this class of systems is that they allow for centralized password verification where the authentication system is shared by many computing systems. However, they have additional risks because of their distributed architecture and because they typically deal with a much larger number of user accounts. Examples of systems in this class are NIS, NIS+, TACACS, RADIUS, etc.

3.2. Criteria

1. The system shall prevent the use of trivial and predictable authenticators. For example, there shall be a configurable complexity requirement for passwords so that they cannot be easily guessed. The system should not allow words that appear in dictionaries of various popular languages to be used as passwords. Passwords should not be the same or anagrams of the User-ID, or simple sequences of characters. [MSC, 2.1.2.2; 11]

2. The system shall not divulge the authenticator (e.g., password, PIN number, token seed, Smartcard seed, etc.) of one user to any other user, including an administrator. [MSC, 2.1.2.2; 1]
3. The authentication information shall not be displayed in clear text¹⁶ (for example, on the screen while it is being keyed in by the user.) [MSC, 2.1.2.2; 2]
4. The system shall allow password and PIN number to be user-changeable at any interval. [MSC, 2.1.2.2; 4]
5. The system shall prompt the user to change the initial password and deny access if the user does not comply. [MSC, 2.1.2.2; 5]
6. Prior to the expiration of authentication information, the system shall provide notification to the user or calling application regarding the imminence of expiration. [MSC, 2.1.2.2; 7]
7. At the time of an attempted password change, the system shall require re-authentication by the user. [MSC, 2.1.2.2; 8]
8. The system shall not enforce the condition of uniqueness on a password¹⁷ between different user accounts. [MSC, 2.1.2.2; 13]
9. Authentication information (e.g. passwords) shall not be sent unencrypted over the network. This will prevent an attacker with a network communications monitoring device from grabbing passwords as users login to their accounts. The system shall have the capability to protect security-related sensitive information from unauthorized disclosure while it is stored and in transit. [MSC, 2.1.4; 1]
10. Even when the password is encrypted, it is possible for an attacker to compromise an account by recording and replaying the login protocol. This attack shall be protected against by using a variable sequence protocol, such as a challenge/response scheme. [MSC, 2.1.2.2; 1]

¹⁶ For example, this implies that, during a login, a password shall not be echoed in clear text. Additionally, any occurrence of a clear text password, encryption key or other authentication information in the memory shall be overwritten immediately after use.

¹⁷ The system shall not prevent a user from unknowingly choosing a password that is already being used by another user. Otherwise the existence of that password would be divulged.

11. An ‘offline’ dictionary attack can be mounted by recording part of the login protocol sequence and then guessing the password that matches the recorded sequence. For example, if the attacker can record the encrypted password, then this can be used to compute the actual password without having to repeatedly contact the authentication server. Therefore, the system shall transmit encrypted authenticators, which will not be extracted by an unauthorized eavesdropper. [MSC, 2.1.2.2; 1]
12. If the authentication protocol involves a PIN¹⁸, this information should be encrypted while being transmitted over the network. [MSC, 2.1.2.2; 1]
13. **DESIRED**: If a server process stays constantly logged-on on a long-term basis (e.g., continuous session), the system should not impose mandatory authentication information aging for such interfaces. [MSC, 2.1.2.2; 10]
14. When password mechanisms are used, the system shall require that the password is configurable to administrator-specified characteristics for minimum password length, minimum alphabetic characters, and minimum numeric or special characters. The default shall be no less than six characters. [MSC, 2.1.2.2; 12]
15. The system shall support minimum and maximum ages for passwords. The system shall offer an authentication information-aging feature, so that users shall be required to periodically change authentication information. [MSC, 2.1.2.2; 6]
16. There shall be a mechanism to prevent the reuse of the authentication information within an administrator-defined period. For example, when updating a password, a user shall be prevented from using a password that was used in the recent past. [MSC, 2.1.2.2; 9]
17. **DESIRED**: The system should have the capability to generate random initial passwords for user accounts. [NEW]
18. **DESIRED**: If passwords are stored in a one-way hashed form, a “salt” should be included. This will reduce the likelihood of a successful pre-computed dictionary attack. [MSC, 2.1.4; 2]

¹⁸ Exception is the use of PINS in ATM transactions, etc. where the ISO standards for PINS must be used

4. Criteria for Trusted Third Party Systems

4.1. Introduction

Trusted Third Party systems improve on the security functionality provided by simple Server based authentication systems. Examples of such systems are the various versions of Kerberos that are currently available. They provide the following additional functions:

- ◆ Strong authentication: The user's password is authenticated without being explicitly presented to the authentication server. This protects the password better and prevents its loss to attackers.
- ◆ Mutual authentication: While the user is being authenticated, the authentication system also proves its validity to the user. This prevents spoofing attacks where a fake authentication system captures a user's authentication information.
- ◆ Peer to peer authentication: This allows 2 tier and 3 tier client-server applications to be secured. The client software can securely forward the user's identity to the server for access control.
- ◆ Single Sign On: Once the user has authenticated himself to the system, this function allows other applications to depend on that action and not require the user to reauthenticate for each application.

4.2. Criteria

1. The system shall be resistant to offline dictionary attacks. One way to secure a Kerberos system against this attack is to use the pre-authentication feature. [NEW]
2. The system shall protect against replay attacks. [MSC 2.1.2.1; 2]
3. To prevent an attack where the KDC¹⁹ is spoofed thereby allowing unauthorized access to a workstation, the workstation login mechanism must authenticate the KDC. [NEW]

¹⁹ Excerpt from comp.protocols.kerberos FAQ: "The term "Kerberos server" generally refers to the Key Distribution Center, or the *KDC* for short. The KDC implements the Authentication Service (AS) and the Ticket Granting Service (TGS). The KDC has a copy of every password associated with every principal. For this reason, it is absolutely vital that the KDC be as secure as possible."

4. The protocol implemented by the system shall conform to RFC 1510, draft 1²⁰. [NEW]
5. The system shall support 3DES-MD5 as one of the cryptographic algorithms. [NEW]
6. The system shall support secure remote administration. [NEW]

²⁰ Reference IETF RFC 1510, "The Kerberos Network Authentication Service (V5)", September 1993, found at: <http://www.ietf.org/rfc/rfc1510.txt>

5. Criteria for Token Based Systems

5.1. Introduction

Tokens refer to portable physical devices that are required during the authentication sequence. The user has to possess a unique physical object to authenticate his identity. This section describes some of the requirements for such devices.

There are two major categories of tokens: memory tokens and microprocessor-based tokens. Memory tokens contain a unique code that identifies them. Examples of memory tokens are bank ATM cards, software licensing ‘dongles’ that plug into a computer’s I/O port, etc. Typically, these devices do not process data; they merely remember identification data in a ROM like memory. Microprocessor based tokens have some kind of computing device within them. They are capable of processing data and evaluating cryptographic algorithms²¹. They can participate in a challenge/response protocol, or generate time-based passwords. In addition, another class of smart tokens follows the ISO standard 7816. These tokens may utilize Public Key based schemes and are covered in section 6.2.

If a token requires that the users authenticate themselves to it in order to activate it, then that authentication sequence should meet the applicable criteria as defined in this profile.

5.2. Criteria

1. The token shall not be forgeable or duplicable. [NEW]
2. The token shall not allow access to the secret authentication information it contains. It should be resistant to physical tampering. When tampering is detected, it should erase its internal information and stop working. [NEW]
3. The authentication protocol used shall be resistant to replay and timing attacks. [NEW]

²¹ Reference FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 140-1 and FIPS 140-2

4. The system shall provide the capability to an administrator to require use of a knowledge-based mechanism (a second factor mechanism), such as a PIN, in conjunction with the token to prevent unauthorized use of the token if it is lost or stolen. If a second factor mechanism is processed by the authentication system, the authentication information must be encrypted at all times. [NEW]
5. If a PIN is sent over the network, the PIN shall be encrypted. [MSC, 2.1.2.2; 1]

6. Criteria for Public Key Systems

6.1. Introduction

Public key systems are a relatively new technology that provides functionality suitable for recent applications.

Typically, there are two authentication steps involved when a user logs in using a public key system. First, the user is required to authenticate themselves so that the correct private key is accessed and (possibly) decrypted. Depending on the authentication technology used here, this step should meet the applicable criteria as defined in this profile. If the public key system uses a hardware token, and that token requires that its users authenticate themselves to it before it can be used, then that authentication sequence should meet the applicable criteria. After the private key is obtained, it is used to authenticate the user to the authentication system. The acceptable criteria for the second step are listed below.

6.2. Criteria

1. The system shall support the x.509 v3 certificate format, and the v2 Certification Revocation List format. [MSC, 2.1.4; 8]
2. The system shall conform to current PKI standards for digital signatures, certificate and CRL formats, OCSP, and interfaces. Some of the standards are PKCS#1, PKCS#7, PKCS #10, PKCS #11. [NEW]
3. The system shall maintain an audit log of all significant events such as; certificate issuance, revocation, CRL signing, and administrative actions. [NEW]
4. The system shall be able to acquire time from a trustworthy time source, such as the U.S. Naval Observatory Master Clock, and use that time for audit trails and system logs. [NEW]
5. Registration Authorities (RA) shall have the option of enrolling the users via manual procedures. [NEW]
6. The system shall have a method to revoke certificates. [NEW]

7. The Administrator shall have the ability to constrain the set of trusted Certificate Authorities that are accepted by users of the system. [NEW]
8. Besides authentication, if the system supports encryption and signing of user data, then it shall use separate keys for each function. For example, a key used for digital signatures shall not be used for encryption purposes. [NEW]
9. **DESIRED**: Duplication of private keys increases the risk of key compromise. The system should allow the export of private keys only in encrypted PKCS#12 form. [NEW]
10. **DESIRED**: The system should warn the user about the risks of duplicating private keys before starting the duplication process. [NEW]
11. **DESIRED**: The system should support the use of hardware that meets FIPS²² 140-1 level 3 standard for all cryptographic computations of the Certificate Authority. [MSC, 2.1.4; 7]
12. **DESIRED**: The system should support key lengths of at least 2048 bits for RSA keys. [MSC, 2.1.2.2; 11]
13. **DESIRED**: If Certificate Revocation Lists (CRLs) are not checked during the certificate verification, then the system should support OCSP²³ to validate certificates. [NEW]

²² Reference: NIST, *Security Requirements for Cryptographic Modules* (<http://csrc.nist.gov/fips/fips1401.htm>)

²³ Online Certificate Status Protocol – Reference The Internet Society's RFC 2560

7. Criteria for Biometrics Systems

7.1. Introduction

Biometrics based authentication systems use a physical attribute of the subject being authenticated. The person does not have to remember a password or carry any special device.

Technology Providers utilizing biometric based authentication systems should supply with the tested product the ratios involved in false detects.

7.2. Criteria

1. The system shall not be possible to spoof the system, even with the cooperation of the authentic subject. For authentication based on the personal characteristics of the user, the system has to minimize the chance of a masquerade attack by an unauthorized user. [MSC, 2.1.2.3; 1]
2. The system shall be resistant to common variations in human attributes, as in the subject having a common cold, or sweaty palms. [NEW]
3. The user's biometrics profile shall be encrypted and protected against accidental or deliberate publication. [MSC, 2.1.4; 2]
4. The system shall conform to the criteria listed in ANSI X9.84. [NEW]
5. The system shall provide the capability to an administrator to require use of a separate security technology, for example a knowledge-based mechanism such as a PIN, in conjunction with the biometric capability. [NEW]

Appendix A: Industry Standards

For the purposes of these criteria, the terms “public and widely-used or financial industry standards” shall refer to the following items, as specified within this document.

Symmetric Encryption algorithms	<ul style="list-style-type: none"> • 3DES (ANSI X9.52, X9.66) • IDEA • RC4 • RC5 • RIPEM
Asymmetric Algorithms (for symmetric key agreement or key transport)	<ul style="list-style-type: none"> • RSA (ANSI X9.44) • D-H (minimum 1024-bit modulus – ANSI X9.42) • ECDH (ANSI X9.63)
Digital hashing algorithms	<ul style="list-style-type: none"> • SHA-1 (ANSI X9.30-2) • MD5
Digital signature algorithms	<ul style="list-style-type: none"> • DSA (ANSI X9.30-1) • rDSA (ANSI X9.31) (includes RSA) • EC-DSA (ANSI X9.62)
Key management standards and protocols	<ul style="list-style-type: none"> • ANSI X9.70, ANSI X9.73, ANSI X9.69, ANSI X9.24, ANSI X9.77 • CMP • PKCS #7 • IETF PKIX standards
Random number generators	<ul style="list-style-type: none"> • ANSI X9.82
Prime number generators	<ul style="list-style-type: none"> • ANSI X9.80
Cryptographic Device Security	<ul style="list-style-type: none"> • ANSI X9.66 • FIPS 140-2
Peer Entity Authentication	<ul style="list-style-type: none"> • ANSI X9.72 • FIPS 196
PIN Security	<ul style="list-style-type: none"> • ANSI X9.8, ANSI X9.86, ANSI X9.87
Biometrics Management and Security	<ul style="list-style-type: none"> • ANSI X9.84

In the event that criteria specify that “only” these standards be supported, “these standards” shall be interpreted to refer to those standards, algorithms, and protocols listed above, as well as other relevant standards approved by the following standards organizations: IETF, ANSI X9, ITU-T, ISO, NIST and IEEE.

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 an acceptable algorithm in place of the unlisted algorithm. Systems that do not have this flexibility will be disqualified from the BITS validation process.

Appendix B: MSC Cross-Reference Matrix

This appendix provides the Master Security Criteria [MSC] cross-references to this Product Profile. It provides a quick reference to criteria which have been identified by the Financial Services Industry as *required* (i.e., mandatory), *desired* (i.e., optional) or “*not applicable*” to this product class. Where appropriate, further comment, clarification and/or rationale is provided for each criterion.

Total Number of Required Criteria:	117
Total Number of Desired ²⁴ Criteria:	37
Total Number of [NEW] ²⁵ Criteria:	58

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.1: Identification			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes “identification” 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.			
2.1.1; 1	Required	2.1.1; 1 2.1.1; 2	• (2.1.1; 2) Applicable to administration of the System
2.1.1; 2	N/A	N/A	
2.1.1; 3	Required	2.1.4; 15	Applicable to administration of the system
2.1.1; 4	N/A	N/A	
2.1.1; 5	Required	2.1.3; 9	Minor variation from MSC: Addition of “...administrator specified...”
2.1.1; 6	Desired	2.1.3; 12	Significant extensions from original MSC reference; note that if the TP product performs this criteria, several “requirements” (i.e. “shalls”) exist within this criteria that are mandatory
[NEW]	Required	2.2.1; 20	(Section: 2.2 User login and logout (Authentication & Disconnect)) – Criteria focuses on

²⁴ For more details, reference “Mandatory and Desired Criteria” (Introduction) section of this document

²⁵ Criteria referenced as [NEW] are items currently not available in MSC Version 1.1. These criteria will be considered for future inclusion to the MSC. [NEW] criteria may be Mandatory or Desired.

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
<p>Section 2.1.1: Identification</p> <p>The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "identification" 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.</p>			
			<p>requirement for all User-IDs to use authentication, however special note is given to <i>anonymous</i> IDs.</p>
[NEW]	Required	2.4.1; 36	<p>(Section: 2.4 Storage of information by the Authentication Server) – Criteria: "If the authentication system uses a database or file system to store information, then the authentication system shall use a unique User-ID to access the database or file system."</p>

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.2: Authentication			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "authentication" as: The system shall offer features to verify the claimed identity of a user before allowing system access to the said user.			
2.1.2.1; 1	N/A	N/A	
2.1.2.1; 2	Required	2.6.4; 75 4.2; 2	<ul style="list-style-type: none"> (2.6.4; 75) Significant extensions/clarification from original MSC reference (4.2; 2) (Section: Criteria for Trusted Third Party Systems): Slight modification from MSC reference
2.1.2.1; 3	Required	2.2.5; 29	Applicable to administration of the system
2.1.2.1; 4	Desired	2.6.2; 70	Slight modification from MSC reference
2.1.2.1; 6	Required	2.4.5; 46	Slight modification from MSC reference; removed "...or loss of data and system integrity." Additional references in this profile: (2.4.4; 41), (2.6.4; 82-83), (2.6.6; 92)
2.1.2.1; 8	Required	2.6.2; 68	Verbatim reference of MSC; Additional references: 2.4.4; 40
2.1.2.1; 9	N/A	N/A	
[NEW]	Required	2.1.2; 3	(Section: 2.1 User Registration and Deletion) – New Criteria: "The system shall support multifactor authentication for the authentication of administrators."
[NEW]	Desired	2.1.2; 4	(Section: 2.1 User Registration and Deletion) – New Criteria: The system should allow for the identity of each user to be independently verified before a new user-ID is issued.
[NEW]	Required	2.2.2; 21	(Section: 2.2 User login and logout (Authentication & Disconnect))– New Criteria: "The system shall not impede the re-authentication of users if so required by the relying parties." Base MSC reference: 2.1.2.1; 5
[NEW]	Required	2.1.4; 16	(Section: 2.1 User Registration and Deletion) – New Criteria: "The system shall not permit a user-ID to exist without authentication information." Base MSC reference: 2.1.2.1; 7
[NEW]	Required	2.3.2; 31	(Section: 2.3 Storage of credentials at client site) – New Criteria: "If the user's private or secret authentication information is stored at the client site, then the users shall have to authenticate themselves before they are allowed to access the information. For example, user authentication shall be required before the users are allowed to access their private key."
[NEW]	Required	2.3.2; 32	(Section: 2.3 Storage of credentials at client site) – New Criteria: "Unattended server processes shall be able to use operating system provided authentication to access the security-related information that they require for their operation."
[NEW]	Required	2.4.2; 37	(Section: 2.4 Storage of information by the Authentication Server) – New Criteria: "If the authentication system uses a database or file system to store information, then access to that data shall require authentication."
[NEW]	Desired	2.7.2; 99	(Section: 2.7 Integration and Usability) – New Criteria: "The system should provide information regarding the identity of the authenticated party to the application or relying party."
[NEW]	Desired	2.7.2; 100	(Section: 2.7 Integration and Usability) – New Criteria: " The system should provide information to the application or relying party regarding the strength of the mechanism used to authenticate a user-ID."
Knowledge- and Possession-Based Mechanisms Requirements			
2.1.2.2; 1	Required Required Required Required Required	3.2; 2 3.2; 10 3.2; 11 3.2; 12 5.2; 5	<ul style="list-style-type: none"> (3.2; 2) Verbatim reference of MSC (3.2; 10) Significant variation from MSC reference; focus on variable sequence logon protocol (such as a challenge/response scheme). (3.2; 11) Significant variation from MSC reference; (3.2; 12) Significant variation from MSC reference; focus on authentication involving a PIN (encryption of PIN). (5.2; 5) Significant variation from MSC reference; "If a PIN is sent over the network,

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.2: Authentication			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "authentication" as: The system shall offer features to verify the claimed identity of a user before allowing system access to the said user.			
			<i>the PIN shall be encrypted".</i>
2.1.2.2; 2	Required	3.2; 3	
2.1.2.2; 3	N/A	N/A	
2.1.2.2; 4	Required	3.2; 4	Variation from MSC reference; Stronger enforcement: <i>"The system shall allow password and PIN number to be user-changeable at any interval."</i>
2.1.2.2; 5	Required	3.2; 5	Slight variation from MSC
2.1.2.2; 6	Required	3.2; 15	Extension to original MSC criteria; New 1 st sentence: <i>"The system shall support minimum and maximum ages for passwords."</i>
2.1.2.2; 7	Required	3.2; 6	Slight modification to MSC reference; addition of "...or calling application..."; Frequently this is not a specific Authentication System function, but is within the realm of an authentication system (i.e. a relying party (application, service, etc)).
2.1.2.2; 8	Required	3.2; 7	Slight modification to MSC reference; removal of "..., as well as re-confirmation of the new password."
2.1.2.2; 9	Required	3.2; 16	
2.1.2.2; 10	Desired	3.2; 13	Criteria identified as DESIRED and therefor grammatical changes are applied; Slight modification to MSC reference; Focus is on "server process" and not to "system"; Intent unchanged
2.1.2.2; 11	Required Desired	3.2; 1 3.2; 12	(3.2; 1) Enhancement to the MSC criteria; Addition of last two sentences: <i>"The system should not allow words that appear in dictionaries of various popular languages to be used as passwords. Passwords should not be the same or anagrams of the User-ID, or simple sequences of characters."</i> (3.2; 12) Significant modification to the MSC reference; Focus is on key lengths (Public Key Systems)
2.1.2.2; 12	Required	3.2; 14	Enhancement of MSC reference; Last sentence added for clarity: <i>"The default shall be no less than six characters."</i>
2.1.2.2; 13	Required	3.2; 8	Enhancement of MSC reference; addition to end of criteria: <i>"...between different user accounts."</i>
Personal Characteristics-Based Mechanism Requirements			
2.1.2.3; 1	Required	7.2; 1	Enhancement of MSC reference. Addition of new first sentence: <i>"The system shall not be possible to spoof the system, even with the cooperation of the authentic subject."</i>
[NEW]	Required	7.2; 2	(Section: 7.2 Criteria for Biometrics Systems) – New criteria for this profile only valid for authentication systems claiming support for biometric authentication: <i>"The system shall be resistant to common variations in human attributes, as in the subject having a common cold, or sweaty palms."</i>
[NEW]	Required	7.2; 4	(Section: 7.2 Criteria for Biometrics Systems) – New criteria for this profile only valid for authentication systems claiming support for biometric authentication: <i>"The system shall conform to the criteria listed in ANSI X9.84."</i> As part of the ANSI X9 (Financial Services Standard), the X9F subcommittee, which is dedicated to information and data security, is developing X9.84 "Biometric Information Management and Security". Referenced documents can be found/purchased at http://www.ansi.org or http://www.x9.org
[NEW]	Required	7.2; 5	(Section: 7.2 Criteria for Biometrics Systems) – New criteria for this profile only valid for authentication systems claiming support for biometric authentication: <i>"The system shall provide the capability to an administrator to require use of a separate security technology, for example a knowledge-based mechanism such as a PIN, in conjunction with the biometric capability."</i>

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.3: Authorization			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "authorization" as: The system shall offer features to support the following restrictions: <ul style="list-style-type: none"> • 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. 			
2.1.3; 1	Required	2.6.3; 71	Applicable to administration of the system
2.1.3; 2	Required	2.2.5; 28	
2.1.3; 3	Required	2.2.3; 22	Applicable to administration accesses to the authentication system. Addition of two <i>qualifying</i> sentences at beginning of this criteria: <i>"The system shall limit the number of failed login attempts. This protects against online dictionary attacks. ..."</i>
2.1.3; 4	Required	2.2.3; 23	Significant modification from MSC reference
2.1.3; 5	Desired	2.2.3; 25	Applicable to administration of the system.
2.1.3; 6	Desired	2.4.6; 56	Significant modification from MSC reference
2.1.3; 7	Desired	2.2.3; 24	Applicable to administration of the system. Significant modifications from MSC reference.
2.1.3; 8	Required	2.2.4; 26	Slight modification to MSC reference; Using "...connection shall be terminated..." versus "...shall be dropped..."
2.1.3; 9	Desired	2.6.6; 96	Slight modification from MSC reference; addition of parenthetical qualification at end: "... <i>(such as IP address and port)</i> "
2.1.3; 10	N/A	N/A	
2.1.3; 11	Required Desired	2.1.3; 7 2.6.3; 73	(2.1.3; 7) Applicable to administration of the system. Significant modification from MSC reference. (2.6.3; 73) Verbatim reference of MSC
2.1.3; 12	N/A	N/A	
2.1.3; 13	N/A	N/A	
2.1.3; 14	N/A	N/A	
2.1.3; 15	N/A	N/A	
2.1.3; 16	N/A	N/A	
2.1.3; 17	N/A	N/A	
2.1.3; 18	N/A	N/A	Note: similar criteria exist for Integrity/Audit purposes: (2.4.4; 43), (2.6.4; 79), (2.7.4; 106)
2.1.3; 19	N/A	N/A	
2.1.3; 20	Desired	2.6.3; 74	Modification to MSC reference; emphasis placed on providing the administrator information to the application or relying party regarding concurrent logons
2.1.3; 21	N/A	N/A	
2.1.3; 22	Required	2.6.3; 72	
[NEW]	Required	2.3.3; 33	(Section: 2.3 Storage of credentials at client site) – New criteria: "User credentials and other sensitive data stored on workstations shall be protected against unauthorized viewing."
[NEW]	Required	2.4.3; 39	(Section: 2.4 Storage of information by the Authentication Server) – New criteria: "If the authentication system uses a database or file system to store information, then access to that information shall be restricted to the authentication system."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.4: Confidentiality			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "confidentiality" 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.			
2.1.4; 1	Required	3.2; 9	Modification to MSC reference; addition of two qualifying statements preceding original MSC reference: "Authentication information (e.g. passwords) shall not be sent unencrypted over the network. This will prevent an attacker with a network communications monitoring device from grabbing passwords as users login to their accounts."
2.1.4; 2	Required Desired Required	2.4.5; 48 3.2; 18 7.2; 3	(2.4.5; 48) Significant difference to MSC reference, however, this criteria captures the original intent of the MSC reference (3.2; 18) Significant difference to MSC reference (7.2; 3) Specific to protection of biometric profile protection
2.1.4; 3	N/A	N/A	
2.1.4; 4	Required Required	2.3.5; 35 2.5.5; 65	(2.3.5; 35) Minor modification to MSC reference: use of "impractical" versus "difficult" in reference to compromise for clarity; intent unchanged (2.5.5; 65) Identical to 2.3.5;35 comment
2.1.4; 5	N/A	N/A	Reference criteria (2.6.4;78)
2.1.4; 6	Required	2.4.5; 47 2.6.4; 77	(2.4.5; 47) Minor modification to MSC reference; intent unchanged; addition of "Appendix A" reference (2.6.4; 77) Identical to 2.4.5;47 comment
2.1.4; 7	Required Desired	2.4.5; 49 6.2; 11	(2.4.5; 49) Minor modification to MSC reference; intent unchanged; additional of last sentence for clarity: "Standard cryptographic algorithms are listed in Appendix A". (6.2; 11) Variation to MSC reference; focus on FIPS 140-1 Level 3 standard and use in PKI systems
2.1.4; 8	Required	6.2; 1	Modification and enhancement to MSC reference; Addition of clarity regarding CRLs; Intent unchanged (expanded): "The system shall support the x.509 v3 certificate format, and the v2 Certification Revocation List format."
2.1.4; 9	Desired	2.4.5; 63	Minor modification from MSC reference; Intent unchanged
2.1.4; 10	Required	2.5.5; 64	Minor modification from MSC reference; use of "keying material" versus "key"; Intent unchanged
2.1.4; 11	Required Required	2.1.3; 8 2.5.3; 60	(2.1.3; 8) Minor modification of MSC reference; use of "keying material" versus "key"; Intent unchanged (2.5.3; 60) Significant modification of MSC reference; intent unchanged, but new emphasis placed on "real time"; criteria: "The system shall have the capability to enforce, in real time, the revocation of a user and the associated keying material as and when requested by the administrator."
2.1.4; 12	Required	2.5.3; 61	Significant modification of MSC reference: "The system shall support dual custody of all encryption keys for the purpose of recovery of encrypted data."
[NEW]	Required	2.1.5; 18	(Section: 2.1 User Registration and Deletion / Confidentiality) – New criteria: "The system shall not reveal the passwords or privileges of a new account to unauthorized staff or users."
[NEW]	Required	2.2.5; 27	(Section: 2.1 User login and logout (Authentication & Disconnect) / Confidentiality) – New criteria: "The password entered by the administrator shall not be displayed while it is being typed in."
[NEW]	Required	2.4.5; 45	(Section: 2.4 Storage of information by the Authentication Server) – New Criteria: "The system shall protect the authentication information database from unauthorized use."
[NEW]	Desired	2.6.2; 69	(Section: 2.6 Authentication Process) – New Criteria: "The system should provide a protected path between it and the objects being authenticated so that the communications cannot be compromised."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.5: Data Integrity			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "data integrity" 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.			
2.1.5; 1	N/A	N/A	
2.1.5; 2	Desired	2.6.1; 67	Modification/enhancement from MSC reference; New wording "...any information received from a network interface by IP address, port number, etc."
2.1.5; 3	N/A	N/A	
2.1.5; 4	Required	2.6.4; 84	Modification to MSC reference; Focus re-wording toward <i>replay attacks</i> : "The system shall provide mechanisms to detect, in real-time, replay attacks that duplicate an authentic message."
2.1.5; 5	N/A	N/A	
2.1.5; 6	N/A	N/A	
2.1.5; 7	Required	2.7.4; 103	Applicable to the authentication system itself; Minor modification to MSC reference: "The system shall have the capability to preserve the integrity of its software and data remotely loaded into the system."
2.1.5; 8	Required	2.4.4; 44	Applicable to administration of the system
2.1.5; 9	Required	2.6.4; 80	
2.1.5; 10	Required Required	2.4.4; 43 2.6.4; 79	(2.4.4; 43) Verbatim to MSC reference (2.6.4; 79) Significant re-write, but intent remains the same as MSC reference
[NEW]	Required	2.3.4; 34	(Section: 2.3 Storage of credentials at client site) – New criteria: "User credentials and other sensitive data stored on workstations shall be protected against unauthorized tampering."
[NEW]	Required	2.4.4; 40	(Section: 2.4 Storage of information by the Authentication Server) – New criteria: "If the authentication system uses a database or file system to store information, then the integrity of that data shall be preserved. It shall not be possible to bypass the authentication system and modify the data."
[NEW]	Required	2.4.4; 41	(Section: 2.4 Storage of information by the Authentication Server) – New criteria: "41. During system restart, authentication information shall be recoverable without loss of data and system integrity."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.6: Audit			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "audit" 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.			
2.1.6; 1	Required	2.4.6; 50	Verbatim of MSC reference
2.1.6; 2	N/A	N/A	
2.1.6; 3	Required	2.4.6; 53	Verbatim of MSC reference
2.1.6; 4	Required Required Required	2.1.6; 19 2.2.6; 30 2.4.6; 51	(2.1.6; 19) Significant difference to MSC reference; This criteria is only one element of a rather encompassing MSC criteria [reference]. (2.2.6; 30) Significant difference to MSC reference; This criteria is a subset of the broader MSC criteria reference (2.4.6; 51) Significant difference to MSC reference; This criteria is a pointer to the broader MSC criteria reference
2.1.6; 5	Required	2.4.6; 52	Significant difference to MSC reference; This criteria is a pointer to the broader MSC criteria reference
2.1.6; 6	Required	2.4.3; 38	Verbatim of MSC reference
2.1.6; 7	Required	2.6.6; 91	Minor modification to MSC reference; Addition of "...shall have the capability to...".
2.1.6; 8	Desired	2.4.6; 57	Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.6; 9	N/A	N/A	
2.1.6; 10	Desired	2.4.6; 58	Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.6; 11	Required	2.6.6; 92	Verbatim of MSC reference
2.1.6; 12	Required	2.4.6; 54	Modification to MSC reference; Additional of second enhancement statement: "Any disabling will be noted in the audit log."
2.1.6; 13	N/A	N/A	
[NEW]	Desired	2.4.6; 55	(Section: 2.4 Storage of information by the Authentication Server / Audit) – New criteria: "If the system is running with the audit log disabled, then there should be a clear and continuous indicator to alert and remind the operator."
[NEW]	Required	6.2; 3	(Section: 6 Criteria for Public Key Systems)– New Criteria: "The system shall maintain an audit log of all significant events such as; certificate issuance, revocation, CRL signing, and administrative actions."
[NEW]	Required	6.2; 4	(Section: 6 Criteria for Public Key Systems)– New Criteria: "4. The system shall be able to acquire time from a trustworthy time source, such as the U.S. Naval Observatory Master Clock, and use that time for audit trails and system logs."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
<p>Section 2.1.7: Data Disposal</p> <p>The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "data disposal" 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.</p>			
2.1.7; 1	N/A	N/A	
2.1.7; 2	Desired	2.6.5; 89	Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.7; 3	N/A	N/A	

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.8: System Integrity			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "system integrity" as: The system shall offer features to support the following functions: <ul style="list-style-type: none"> • 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. 			
2.1.8; 1	Desired	2.6.6; 93	Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.8; 2	Required	2.6.4; 76	Significant modification from MSC reference: <i>"76. The system shall be implemented with proper boundary checking so that buffer overflow conditions are not possible."</i>
2.1.8; 3	Required	2.6.6; 94	Applicable to administration of the system
2.1.8; 4	Desired	2.6.4; 87	Applicable to administration of the system; Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.8; 5	Required	2.6.4; 82	Verbatim of MSC reference
2.1.8; 6	Required	2.6.4; 83	Modification to MSC reference; remove of <i>"...or a recover."</i> [and subsequent footnote]
2.1.8; 7	Required	2.7.4; 106	Verbatim of MSC reference
2.1.8; 8	Desired	2.7.6; 109	Applicable to administration of the system; Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
[NEW]	Required	2.1.4; 16	<i>(Section: 2.1 User Registration and Deletion) – New criteria: "The system shall not permit a user-ID to exist without authentication information."</i>
[NEW]	Desired	2.1.4; 17	<i>(Section: 2.1 User Registration and Deletion) – New criteria: "The system should not allow an administrator to create a user-ID that was recently deleted, unless the administrator explicitly overrides the system."</i>
[NEW]	Required	2.4.4; 42	<i>(Section: 2.4 Storage of information by the Authentication Server) – New criteria: "The system shall have the capability to be recovered back to a known earlier state. This operation shall require proper authorization."</i>
[NEW]	Required	2.5.4; 62	<i>(Section: 2.5 Key and Password Management)– New Criteria: "An Authentication Key shall not be used for data encryption purposes."</i>
[NEW]	Required	2.6.4; 78	<i>(Section: 2.6 Authentication Process)– New Criteria: "If the system uses a random number generator, then the algorithm used shall be verified to be secure"</i>
[NEW]	Required	2.7.4; 104	<i>(Section: 2.7 Integration and Usability) – New Criteria: "The security functionality provided by the system shall be resistant to attacks on external infrastructure components the authentication system itself requires, such as DNS, NTP, etc."</i>

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.9: Security Administration			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "security administration" as: The system shall offer features to selectively authorize a highly privileged user (a security administrator) to perform day to day activities such as: <ul style="list-style-type: none"> • 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; • Manage user accounts. 			
2.1.9; 1	Required	2.6.1; 66	Verbatim of MSC reference
2.1.9; 2	N/A	N/A	
2.1.9; 3	Desired	2.6.6; 95	Modification from MSC reference; Removal of reference to "...one or more interfaces..."
2.1.9; 4	N/A	N/A	
2.1.9; 5	N/A	N/A	
2.1.9; 6	Required	2.7.3; 102	Applicable to administration of the system; Slight modification from MSC reference
2.1.9; 7	Required	2.6.6; 90	Modification from MSC reference; "The system shall provide access to authorized individuals to enable the retrieval, copying, printing, deletion and upload of an audit log.
2.1.9; 8	Required	2.7.3; 101	Verbatim of MSC reference
[NEW]	Required	2.1.3; 5	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "The system shall allow only authorized administrators to create or delete user-IDs."
[NEW]	Required	2.1.3; 6	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "The system shall have the capability to activate a previously created credential."
[NEW]	Desired	2.1.3; 10	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "User-IDs related to human users should be configurable (i.e. individually, by groups or all User-IDs) so that they expire after an administrator specifiable period (for example, 6 months.) User-IDs associated with non-human objects (e.g., production batch jobs, servers, routers, etc.) may be excluded from this requirement."
[NEW]	Desired	2.1.3; 11	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "User-IDs that expire should be renewable via a secure re-enrollment procedure"
[NEW]	Desired	2.1.3; 13	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "The system should allow only administrators to suspend and restore User-IDs."
[NEW]	Desired	2.1.3; 14	(Section: 2.1 User Registration and Deletion / Access Control) New criteria: "The system should allow delegation of administrative authority so that specific administrative accounts may have authority over subsets of user accounts. Further, it should be possible to delegate only subsets of authority to some administrator accounts."
[NEW]	Required	2.5.2; 59	(Section: 2.5 Key and Password Management / Authentication) New Criteria: "If the system allows administrators to set user's passwords for new or reinstated accounts, it shall require that users change these passwords when the account is next used before further system access is allowed."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.10: Guidance			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "guidance" as: The vendor shall supply the following product support capability: <ul style="list-style-type: none"> • 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. 			
2.1.10; 1	Required	2.7.4; 107	Significant difference to MSC reference; This criteria is a pointer to the broader MSC criteria reference; Intent unchanged
2.1.10; 2	N/A	N/A	

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.1.11: Non-Repudiation			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.1] recognizes "non-repudiation" 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.			
2.1.11; 1	Desired	2.6.4; 85	Modification from MSC reference; Criteria is identified as DESIRED; replaced "...authenticity and integrity to record" with "...securely record..."; Also, addition of parenthetical reference of "(administrator)"
2.1.11; 2	Desired	2.6.4; 86	Criteria identified as DESIRED; this is a verbatim reference to the MSC other than grammatical changes necessarily to create DESIRED versus "mandatory".
2.1.11; 3	N/A	N/A	
2.1.11; 4	N/A	N/A	
[NEW]	Required	6.2; 2	(Section: 6.2 Criteria for Public Key Systems) New criteria: "The system shall conform to current PKI standards for digital signatures, certificate and CRL formats, OCSP, and interfaces. Some of the standards are PKCS#1, PKCS#7, PKCS #10, PKCS #11."; This criteria is closely associated with several "Confidentiality" and "Integrity" criteria and Appendix A.
[NEW]	Required	6.2; 8	(Section: 6.2 Criteria for Public Key Systems) New criteria: "8. Besides authentication, if the system supports encryption and signing of user data, then it shall use separate keys for each function. For example, a key used for digital signatures shall not be used for encryption purposes."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.2: Functionality			
The BITS Financial Services Security Lab Security Criteria Framework [SCO, 2.1.2] describes "Functionality" as: Functional criteria are applied to assess the strength of security features. In addition, the testing will focus on an analysis of the security functions that the product was designed to perform (e.g., Firewall product performing traffic filtering). Depending on the product tested, the criteria may or may not include reliability criteria. Reliability criteria are applied to evaluate the redundancy, recovery, and intrusion (inserted faults) tolerant aspects of the product design, and may include criteria for such things as tolerance to a single intrusive event in redundant units or tolerance to multiple intrusions.			
2.2; 1	N/A	N/A	Note: Criteria is not directly referenced in this profile, however, Appendix A provides a list of public and widely-used or financial industry standards.
2.2; 2	N/A	N/A	
2.2; 3	N/A	N/A	
2.2; 4	Required	2.7.4; 105	Modification/enhancement to MSC reference; inclusion of second and third [clarity] statements: <i>"For example, the terminology used in various administration screens should be consistent. The behavior of similar or related functions should be consistent."</i>

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.3: Usability			
2.3; 1	N/A	N/A	
2.3; 2	Required	2.7.1; 97	Verbatim reference of MSC
2.3; 3	N/A	N/A	
2.3; 4	Required	2.7.4; 108	Applicable to administration of the system; Addition of parenthetical reference (i.e. "(for administrators)") for clarity
2.3; 5	N/A	N/A	
2.3; 6	Required	2.7.1; 98	Verbatim reference of MSC
2.3; 7	Required	2.6.5; 88	Verbatim reference of MSC

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Section 2.4: Scalability			
2.4; 1	Required	2.6.4; 81	Verbatim reference to MSC

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Criteria for Passive Authentication Systems (Section 3)			
These criteria are not cross-referenced to the current MSC.			
[NEW]	Desired	3.2; 17	New criteria: "The system should have the capability to generate random initial passwords for user accounts."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Criteria for Trusted Third Party Systems (Section 4)			
These criteria are not cross-referenced to the current MSC.			
[NEW]	Required	4.2; 1	New criteria: "The system shall be resistant to offline dictionary attacks. One way to secure a Kerberos system against this attack is to use the pre-authentication feature."
[NEW]	Required	4.2; 3	New criteria: "To prevent an attack where the KDC is spoofed thereby allowing unauthorized access to a workstation, the workstation login mechanism must authenticate the KDC."
[NEW]	Required	4.2; 4	New criteria: "The protocol implemented by the system shall conform to RFC 1510, draft 1."
[NEW]	Required	4.2; 5	New criteria: "The system shall support 3DES-MD5 as one of the cryptographic algorithms."
[NEW]	Required	4.2; 6	New criteria: "The system shall support secure remote administration."

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Criteria for Token Based Systems (Section 5)			
These criteria are not cross-referenced to the current MSC.			
[NEW]	Required	5.2; 1	New criteria: <i>"The token shall not be forgeable or duplicable."</i>
[NEW]	Required	5.2; 2	New criteria: <i>"The token shall not allow access to the secret authentication information it contains. It should be resistant to physical tampering. When tampering is detected, it should erase its internal information and stop working."</i>
[NEW]	Required	5.2; 3	New criteria: <i>"The authentication protocol used shall be resistant to replay and timing attacks."</i>
[NEW]	Required	5.2; 4	New criteria: <i>"The system shall provide the capability to an administrator to require use of a knowledge-based mechanism (a second factor mechanism), such as a PIN, in conjunction with the token to prevent unauthorized use of the token if it is lost or stolen. If a second factor mechanism is processed by the authentication system, the authentication information must be encrypted at all times."</i>

Master Security Criteria (MSC) Reference	Required, Desired or N/A	Authentication Systems Profile Reference	Comment or Rational
Criteria for Public Key Systems (Section 6)			
These criteria are not cross-referenced to the current MSC.			
[NEW]	Required	6.2; 5	New Criteria: <i>"Registration Authorities (RA) shall have the option of enrolling the users via manual procedures."</i>
[NEW]	Required	6.2; 6	New Criteria: <i>"The system shall have a method to revoke certificates."</i>
[NEW]	Required	6.2; 7	New Criteria: <i>"The Administrator shall have the ability to constrain the set of trusted Certificate Authorities that are accepted by users of the system."</i>
[NEW]	Desired	6.2; 9	New Criteria: <i>"Duplication of private keys increases the risk of key compromise. The system should allow the export of private keys only in encrypted PKCS#12 form."</i>
[NEW]	Desired	6.2; 10	New Criteria: <i>"The system should warn the user about the risks of duplicating private keys before starting the duplication process."</i>
[NEW]	Desired	6.2; 13	New Criteria: <i>"If Certificate Revocation Lists (CRLs) are not checked during the certificate verification, then the system should support OCSP to validate certificates."</i>

Appendix C: Bibliography

- MSC *Master Security Criteria (v1.1)*, BITS, February 2000
- SCO *Security Criteria Overview (v1.0)*, BITS, 1999

Appendix D: Glossary of Terms

Definitions provided in this document are provided via references in various books and publications. Several of these references are included at the end of this section.

TERM	DEFINITION
access control	<i>A mechanism for limiting use of some 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 which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files [3]</i>
administrator	<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 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>
AIS	<i>Automated Information System - 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>
API	<i>Application Programming 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, Smart card seed, etc.</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>This happens when more data is put into a buffer or holding area, then the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This 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 containing 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 over 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 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>Typically an “offline attack” or “brute force attack” ... this is the process of “guessing” passwords, based on a set of key words or characters, until a match is made.</i>
digital signature	<i>A method based on public key encryption to verify identities over a network</i>
DLL	<i>Dynamic Link Library - 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>
DNS	<i>Domain Name System - 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>
end user	<i>Taken 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>
encrypt	<i>To scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption)</i>
escrow	<i>To hold something in safekeeping. Most uses of the word actually mean keeping the something safe from the owner as opposed to providing any safety for the owner</i>
group	<i>A named collection of users, created for convenience in stating authorization policy</i>
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>
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>

TERM	DEFINITION
log	<i>To record an action [2]</i>
log file	<i>A file that lists actions that have occurred [2]</i>
MAC	<i>Message Authentication Code – a synonym of message integrity code (MIC) [1]</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>
MIC	<i>Message Integrity Code – 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 and the third party can independently verify the source [1]</i>
NTP	<i>Network Time Protocol</i>
OCSP	<i>Online Certificate Status Protocol</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 one time [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>
passive attack	<i>Attack which 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>
PIN	<i>Personal Identification Number – a short sequence of digits used as a password [1]</i>
PKCS	<i>Public Key Cryptography Standards (PKCS) ... 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>
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 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 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 as is necessary or convenient [1]</i>

TERM	DEFINITION
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 of 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 when implying that the entity doing the reply of messages is mounting some sort of security attack</i>
repudiation	<i>Denying that you did something or made some statement [1]</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-relevant functions, mechanisms, and characteristics of AIS hardware and software [3]</i>
server	<i>Some resource available on the network to provide some 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, some message</i>
signature	<i>A quantity associated with a message which only someone with knowledge of your private key could have generated, but which can verified through knowledge of your public key [1]</i>
spoof	<i>To convince someone that you are some entity X when you are not X, without X's permission [1]</i>
strong authentication	<i>Techniques that permit entities to provide evidence that they know a particular secret without revealing the secret. [6]</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. [SCO 2.1.1]</i>
system administrator	<i>In the scope of this profile, an individual (user) having higher privilege at the operating system level.</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>Taken into 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 which is unique to a particular user of a computer or group of computers which share user information. The operating system uses the uid to represent the user in its data structures, e.g. the owner of a file or process, the person attempting to access a system resource etc.</i>
X.509	<i>A CCITT standard for security services within the X.500 directory services framework. The</i>

TERM	DEFINITION
	<i>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
- ◆ [6] J.J. Tardo and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates." In Proc IEEE Symp. Research in Security and Privacy . IEEE CS Press, 1991.