ACCESS CONTROL IN SUPPORT OF INFORMATION SYSTEMS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 3

29 October 2010

Developed by DISA for the DoD

This page is intentionally blank.

-

TABLE OF CONTENTS

Page

SUMMARY OF CHANGES IX

1. INTRODUCTION 1

1.1 Background 1
1.2 Authority 2
1.3 Scope 3
1.4 Writing Conventions 3
1.5 Vulnerability Severity Code Definitions 4
1.6 STIG Distribution 5
1.7 Document Revisions 5

2. ACCESS CONTROL LAYERS 7

2.1 The Access Control Perimeter 8
2.1.1 Asset Container Perimeter 9
2.1.1.1 Physical Asset Containers 10
2.1.1.2 Logical Asset Containers 10
2.1.2 Workplace Perimeter 12
2.1.2.1 Secure Rooms 13
2.1.3 Facility/Building Perimeter 13
2.1.4 Installation Perimeter 13

3. ACCESS CONTROL METHODS 15

3.1 Identification Credentials 16
3.2 Personal Authentication 18
3.3 Authorization 18
3.4 Logical Access Control Methods 20
3.4.1 Techniques for Security Network Access 22
3.4.1.1 Network Architecture Controls 22
3.4.1.2 Remote Network Access 23
3.4.1.3 Securing Network Ports 24
3.4.1.3.1 Physical Security for SIPRNeT Ports 24
3.4.1.3.2 Logical Network Port Security 25
3.4.1.3.3 Port Authentication Using 802.1X 26
3.4.1.4 Network Access Control (NAC) Systems 28
3.4.2 Cryptography 29
3.4.2.1 Encryption 30
3.4.2.2 PKI Compliance Requirements 32
3.4.3 Passwords , PINs, and Implementations of Something You Know 35
3.4.4 Hardware Tokens 37
3.4.4.1 The DoD Common Access Card 38
3.4.4.2 Alternate Login Token 40
3.5 Physical Access Control Methods 41
3.5.1 Classified Storage and Handling 41

3.5.2 Attended Access ... 42
3.5.3 CAC and DBIDS for Physical Access Control ... 43
3.5.4 Supplemental Badges, Memory Cards, and Smart Cards ... 43
3.5.4.1 Badges ... 44
3.5.4.2 Memory Cards ... 45
3.5.4.3 Smart Cards ... 45
3.5.5 PINs, Combinations, and Other Forms of Something You Know ... 46
3.5.6 Physical Tokens ... 47
3.5.7 Physical Intrusion Detection Systems ... 48
3.5.8 Other Physical Security Considerations ... 48

4. BIOMETRIC SYSTEMS ... 51

4.1 Biometric Technology and Terminology ... 51
4.1.1 Identification versus Verification ... 52
4.1.2 Enrollment ... 53
4.1.3 Verification ... 53
4.2 Separation of Duties ... 54
4.3 Protecting the Enrollment Process ... 55
4.3.1 Verification of Identification during Enrollment ... 55
4.3.2 Quality Control of the Reference Templates ... 56
4.3.3 Guarding against Modification of the Reference Templates ... 58
4.4 Protecting the Verification Process ... 58
4.4.1 False Acceptance Rate (FAR) Configuration ... 58
4.4.2 Anti-Spoofing Techniques ... 59
4.4.3 Residual Image Check ... 60
4.4.4 Limitation on Unsuccessful Authentication Attempts ... 60
4.4.5 Protection against Bypass and Replay ... 61
4.5 Fallback and Override Requirements ... 62
4.5.1 Fallback Procedures ... 62
4.5.2 Override Procedures ... 63
4.6 Cryptographic Controls ... 63
4.7 Monitoring and Auditing the Biometric System ... 65
4.8 Physical Security of the Biometric Components ... 66

5. ACCESS CONTROL INTEGRATION ... 67

5.1 Assessing the Value of the Asset ... 68
5.2 Risk Analysis ... 68
5.2.1 Compliance Assessment Tools ... 69
5.3 Determining the Access Control and Asset Container Perimeters ... 71
5.4 Determining Technical Requirements ... 72
5.5 Integrating Access Control Methods ... 73
5.5.1 Combining a Hard Token and a PIN ... 73
5.5.2 DoD-approved PKI ... 73
5.5.3 Combining a Hard Token and Biometrics ... 74
5.5.4 Combining a PIN and Biometrics ... 74
5.5.5 Three-Factor Authentication ... 75
5.5.6 Multiple Uses of the Same Authentication Factor ... 75

5.6 Access Control Decision Matrix 76

APPENDIX A. RELATED PUBLICATIONS 79

APPENDIX B. MISSION ASSURANCE CATEGORIES AND CONFIDENTIALITY LEVELS 81

APPENDIX C. LIST OF ACRONYMS 83

This page is intentionally blank.

TABLE OF FIGURES

Page

Figure 2-1. Layered Protection of Assets 7
Figure 2-2. Potential Access Control Perimeters 9
Figure 2-3. Layered Protection of Logical Asset 11
Figure 3-1. Example of Leveraging of Logical Security Sevices 21
Figure 3-2. Example 802.1X Implementation 27
Figure 3-3. Generic Depiction of CAC Layout 39

TABLE OF TABLES

Table 1-1. Vulnerability Severity Code Definitions 4
Table 5-1. Vulnerability Assessment Checklists and Tools 70
Table 5-2. Personal Authentication Methods 77

This page is intentionally blank.

SUMMARY OF CHANGES

GENERAL CHANGES – 29 October 2010

The previous release was Version 1, Release 2, 26 December 2008.

SECTION CHANGES

SECTION 3. ACCESS CONTROL METHODS

- 3.4.2. Removed misleading statement in last paragraph, first sentence: "... and has a limitation that the amount of data to be encrypted cannot be longer then the length of the key itself." Replaced with text that explained that Asymmetric keys are not typically used to encrypt large amounts of data because the ciphers are slow and processing intensive.

GENERAL CHANGES – 26 December 2008

The previous release was Version 1, Release 1, 17 October 2007.

SECTION CHANGES

SECTION 1. INTRODUCTION

- Minor grammar and spelling corrections made based on input from various users.

SECTION 2. ACCESS CONTROL LAYERS

- Minor grammar and spelling corrections made based on input from various users.
- Corrected appendix number in DoD 5200.1-R.

SECTION 3. ACCESS CONTROL METHODS

- Minor grammar and spelling corrections made based on input from various users.
- 3.4.1.3.1. Added "and MAC address filtering" and clarified requirement. The previous text generated many questions as it was unclear.
- (AC34.030: CAT III). Added the words "logical" and "using MAC filtering" to clarify the policy in response to input from various users.

SECTION 4. BIOMETRIC SYSTEMS

- Minor grammar and spelling corrections made based on input from various users.

SECTION 5. ACCESS CONTROL IMPLEMENTATION SOLUTIONS

- Minor grammar and spelling corrections made based on input from various users.
- Section 5.3, corrected appendix number in DoD 5200.1-R.
- Section 5.5, major change to second paragraph. Text starting with “Although” to the end of the paragraph added to explain current DoD policy gap for three-factor authentication with regard to highly critical or sensitive systems. Discusses best practices and use of three-factor authentication for protection of classified systems.

APPENDIX A. RELATED PUBLICATIONS

- Reference information and links updated.
- Added link for TSA Qualified Products List for biometrics.

APPENDIX B. IAVM COMPLIANCE

Not updated.

APPENDIX C. MISSION ASSURANCE CATEGORIES AND CONFIDENTIALITY LEVELS

Not updated.

APPENDIX D. LIST OF ACRONYMS

Not updated.

1. INTRODUCTION

This Access Control in Support of Information Systems Security Technical Implementation Guide (STIG) details a security framework for use when planning and selecting access control for protecting sensitive and classified information in the Department of Defense (DoD). It provides a consolidated starting place for the security planning team responsible for ensuring compliance with DoD access control policies related to the protection of information technology (IT) assets, including associated data, hardware, software, and communications. In support of a discussion of the security framework, a discussion of the various types of logical and physical access control techniques is provided. The relative strengths and appropriate usage of these various access control methods are emphasized.

1.1 Background

This STIG provides background and context for access control issues including the process of identification, authentication, and authorization for access to protected assets. In many access control solutions, users are often required to authenticate again and again as they traverse physical and/or logical security layers to gain access to an asset or request access to additional resources. This procedure inconveniences the user and, more importantly, often does not result in increased assurance and may decrease user cooperation, thereby increasing risk. Thus, the STIG presents a practical methodology for selecting and integrating logical and physical authentication techniques while tying the solution to the asset's value, environment, threat conditions and operational constraints. The solution must protect access to restricted assets while considering the need for appropriate and authorized access for DoD personnel, contractors, and coalition forces.

This guidance supports DoD's implementation of the Government's mandate for an inter- and intra-agency solution for both establishing identity and consistent application of appropriate levels of assurance (LoA) for Federally controlled information systems. *OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies* and *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems* address a graduated and appropriate application of access control while HSPD 12 addresses the need for standardization of identity credentials across Federal Agencies.

OMB 04-04 and Federal Information Processing Standards (FIPS) 199 provide a framework and standards for categorizing information and information systems to meet the security objectives of confidentiality, integrity, and availability. These standards seek to address the inconsistent application of security controls as information was shared across agency and third party boundaries. FIPS 199 provides a standard framework for government-wide use in information designation while OMB M-04-04 describes assurance levels for authentication by type for electronic transactions.

Homeland Security Presidential Directive (HSPD) 12 addresses a consistent identity credential while leaving the access control uses of that (or other credentials) to the local level. FIPS 201 provides guidance for implementation of HSPD 12. FIPS 201 defines the Personal Identity Verification (PIV) card, which is a cryptographically enabled smart card. Although many vendors may claim compliance with HSPD 12 or FIPS 201, sites should be aware that use of

smart card technology requires implementation of standardized processes as well as the required technology, including an adjudicated National Agency Check (NAC-I).

The DoD will be migrating the current Common Access Card (CAC) to be the DoD's implementation of the requirements of HSPD 12 and FIPS-201. DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12 as well as a primary component of layered protection for national security systems. Identity-proofing, issuing, and managing the CAC is not the responsibility of individual system owners. System owners are, however, responsible for appropriately using the physical and logical access credentials provided on the CAC.

NOTE: Throughout this document, where the DoD CAC is used, the implication is that the HSPD 12 compliant and approved solution for other government agencies, when available, will also be accepted if authorized by the data owner.

To improve information assurance and standardize access control solutions, DoD has mandated the use of approved digital certificates for authenticating to DoD networks, web servers, and signing/encrypting email. Certificates issued by the DoD Public Key Infrastructure (PKI) to individuals will primarily be issued on the CAC. However, certificates may also be issued by DoD-approved external PKIs for use in authenticating to web servers. These certificates won't be on the CAC. While it is easy to confuse the CAC and PKI, implementers and policy makers must bear in mind that it is PKI that is mandated for use in logical access solutions. As discussed in later sections, the CAC represents the merger of the DoD ID card and the PKI program. Placing the certificate on the CAC rather than the host or client increases the level of assurance. This standardized solution will also enable users to access multiple physical and logical assets without the need to for multiple locally issued credentials and authentication tokens.

Security Managers should use this STIG as a starting point for evaluating access control solutions but must also reference the appropriate policy guidance for specific policies when implementing these physical security techniques as part of the access control solution. This document provides a perspective on how information technology solutions can be used either in place of or in combination with physical security techniques to provide appropriate protection for DoD assets. Section 2 provides an overview of access control terms and introduces the layered approach required when planning and implementing access control solutions. Section 3 gives an overview of asset protection technologies and provides policies for implementation of these protection mechanisms. Section 4 provides requirements for securing biometric systems, replacing the previously published Biometric STIG. Section 5 describes the methodology and considerations for selecting appropriate access control solutions by providing recommended steps and tables showing options available given particular asset values.

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination

with Director, National Security Agency (NSA)." This document is provided under the authority of DoD Directive 8500.1.

This document also provides supplementary information and guidance for IAOs and other responsible Security Managers regarding physical access controls. This guidance is consistent with the policies of DoD 5200.1-R and 5200.8-R. This information is provided in support of the stated purpose of the Access Control STIG, which is to facilitate the integration of logical and physical security controls in protecting information systems and data assets. Users must consult these regulations and other STIGs as the specific technology and architecture used dictates.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at Public, Sensitive, and Classified confidentiality levels for any Mission Assurance Category (MAC) level.

1.3 Scope

This guide implements DoD access control and information assurance requirements as stated in DoDD 8500.1, DoDI 8500.2, and DoDI 8520.2. This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (Sas) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts by providing guidance on integrated access control solutions. Integrated access control solutions are generally best if designed by a multi-disciplined team. This team should consist of representatives from any or all of the following areas:

- The data owner or designated representative
- The IAO or responsible information security manager
- The responsible physical Security Manager
- Host installation security representatives
- GSA representative (if the facility is GSA-owned)
- Civilian police officials, as applicable

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Severity Category Codes (CAT) are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

Table 1-1. Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

For access control, policies are marked as CAT I if failure to comply may lead to an exploit which: has a high probability of occurring; does not require specialized expertise or resources; and leads to unauthorized access to high value information (e.g. Classified). Exploitation of CAT I vulnerabilities allow an attacker physical or logical access to a protected asset, allows privileged access, bypasses the access control system, or allows access to high value assets (e.g. Classified). CAT I vulnerabilities include allowing access to the access control system administrative password, or failure to perform identity-proofing prior to badge issuance.

Exploitation of CAT II vulnerabilities also leads to unauthorized access to high value information; however, additional sophistication, information, or multiple exploitations are needed. Exploitation of CAT II vulnerabilities provides information that has a high potential of allowing access to an intruder but requires one or more of the following: exploitation of additional vulnerabilities; exceptional sophistication or expertise; or provides direct or indirect access to high value information (e.g. Classified).

An access control policy with a CAT III severity code requires unusual expertise, additional information, multiple exploitations, and does not directly or indirectly result in access to high value information. Exploitation of CAT III vulnerabilities provide information that potentially

could lead to compromise but requires additional information or multiple exploitations, but does not provide direct or indirect access to high value information.

1.6 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site located at http://iase.disa.mil. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally blank.

2. ACCESS CONTROL LAYERS

An access control method protects systems, resources, or information assets by allowing authorized access and/or detecting and deterring unauthorized access. Some access control methods may also validate the level of authorization or need-to-know for an authenticated user. Assets can be physical or logical. Physical assets may include items such as classified written material, buildings, equipment, or personnel. Logical assets may include items such as intellectual property or electronically stored privacy act and sensitive or classified data.

An effective security solution proactively implements access control methods using a holistic rather than a reactive, bit-by-bit approach. The solution should leverage information about the asset and its environment and provide defense-in-depth (also known as security-in-depth) using layered security techniques. This layered approach calls for an integrated solution combining complementary security controls at a sufficient level to deter and detect unauthorized entry and activity within the facility or logical system. Figure 2-1, Layered Protection of Assets, illustrates the concept of a layered or security-in-depth approach for the protection of an asset. Note that not all asset environments will have every layer, as explained in subsequent sections of this document.

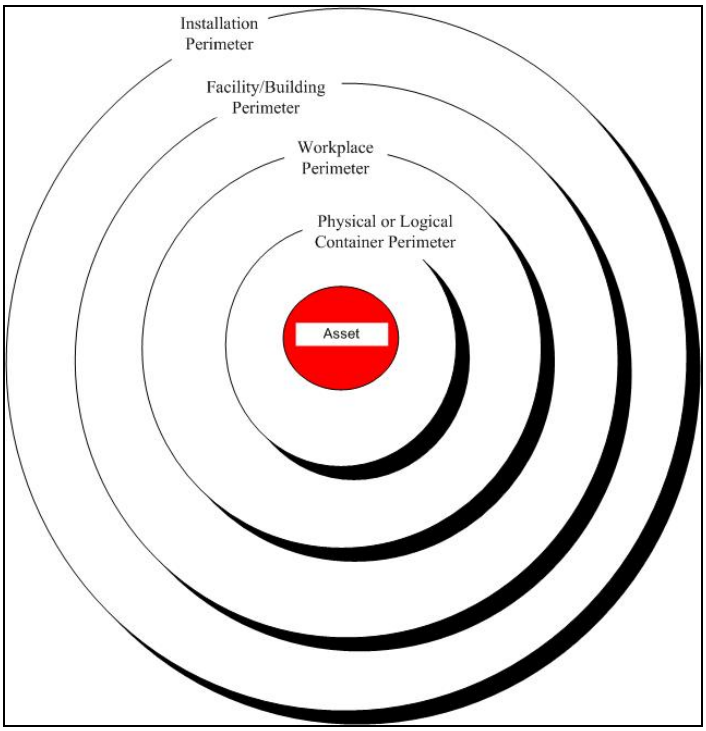

Figure 2-1. Layered Protection of Assets

NOTE: Used with permission of author as noted in Appendix A.

Since it is impossible to design the perfect security solution at each layer, gaps or vulnerabilities are mitigated by the strengths at other layers. The LoA of the access control solution increases with the use of multiple access control techniques used together or at various security boundaries (perimeters) of the access process. Additionally, the LoA is also generally increased when the

methods offering greatest personal authentication assurance are closest to the asset being protected. For this reason, use of a combination of both physical and logical controls is employed in DoD to protect access to high value assets.

Threats to assets stem from two general categories: catastrophic events such as natural disasters and events caused by humans. The catastrophic threat is not the main focus of this document but is very important when planning for business continuity. The threat to assets from adverse human behavior can come from an insider or outsider. Thus, allowing authorized access must include methods for: identification, authentication, authorization, and auditing. These steps will result in a robust solution with an appropriate level of assurance that the system is accessed by authorized users who have a validated need-to-know.

Access control must include detection of and initial response to successful and unsuccessful access by unauthorized entities. Additionally, a disaster recovery plan must be in place to ensure mission continuity and recovery for mission essential systems. Procedures for both incident handling and disaster recovery must include process reassessment and improvement. Large, bulky and cumbersome procedural documents should be avoided or supplemented with checklists as these are emergency documents. Training of users and key personnel are also essential to the success of incident and contingency planning. The format and structure of contingency plans may differ based on mission requirements.

The same process of determining assets, risk levels, and applying the security framework applies to both tactical and non-tactical environments. Identifying potential threats and the level of protection required for the assets are necessary. Commanders must also identify and mitigate additional risks which may be unique to the specific tactical environment.

2.1 The Access Control Perimeter

An access control perimeter is a layer of physical or technical elements used to permit or deny access to or from a restricted area or system. The outer access control perimeter is the physical or logical point where users first encounter access control. This outer perimeter can occur at any point in the security layer depicted in Figure 2-1 and is determined by a multi-disciplined team as described in Section 1.3. An access control point (ACP) is the point where users are either allowed or denied access. A perimeter may have multiple ACPs, each point should be controlled using appropriate methods as discussed in later sections of the document.

Figure 2-1, Layered Protection of Assets, depicts the layers applicable to the DoD environment. However, not all layers are present or relevant for all assets. Asset protection must start with an evaluation of the asset being protected and build outward from the asset. The purpose of the access control system must be clearly defined with respect to the asset being protected. An assessment of the asset’s value, type, and the known tactics, which may be used to gain unauthorized access or damage the asset, is an important step. Another challenge is the determination of where the outermost access control perimeter must be placed. This decision is based upon DoD policy governing the protection of the specific type and value of an asset as discussed in other sections.

Using the access control security framework, the security team can appropriately combine and implement security techniques at the ACPs of the Asset Container Layer and the ACP of the outer access control perimeter. Figure 2-2, shows a fixed-base example of the various points where security could be implemented using the layered approach depicted in Figure 2-1.

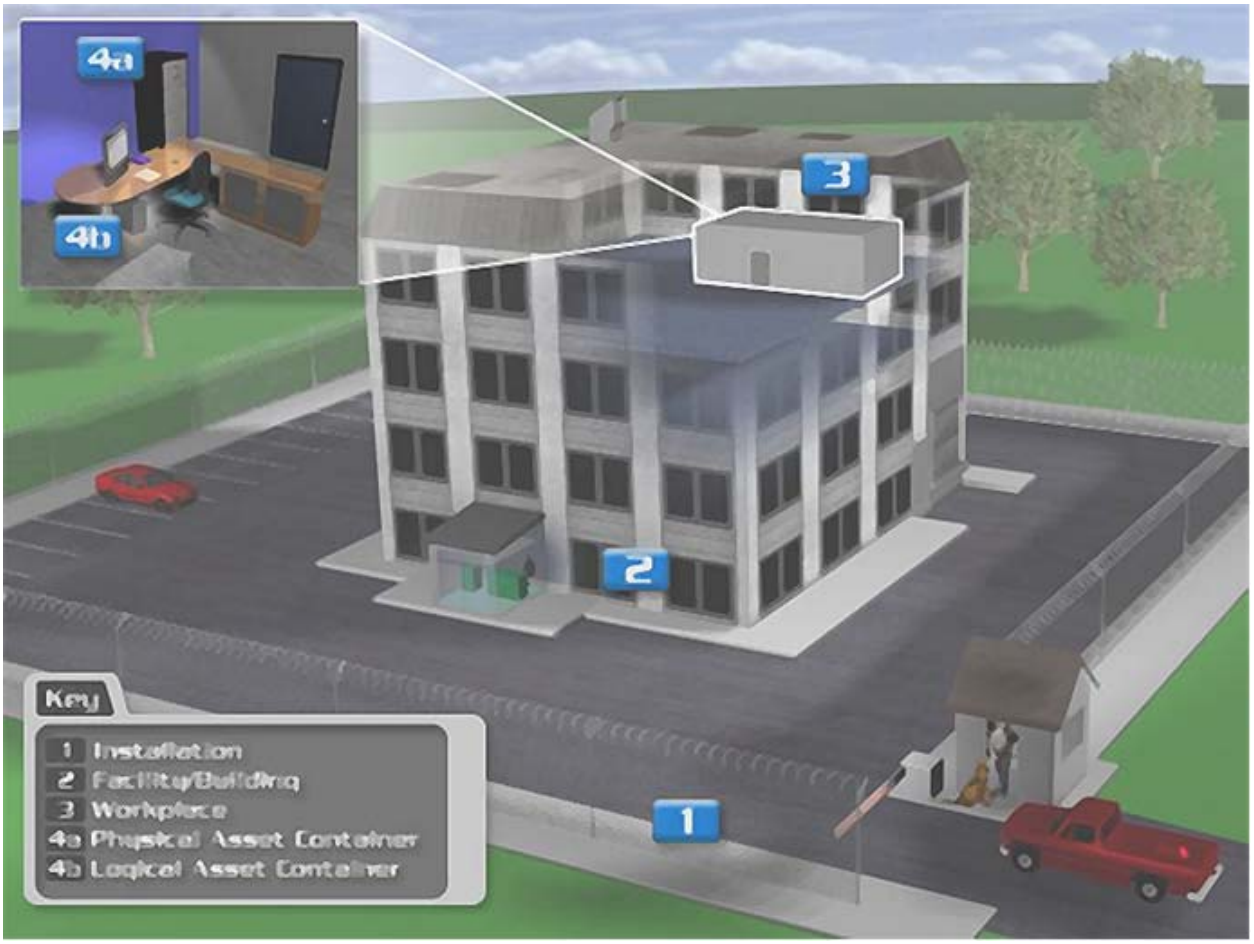

Figure 2-2. Potential Access Control Perimeters

The following subsections define each security layer and outlines potential issues and considerations for each layer. Special issues relating to selection of the layer as the outermost access control perimeter are also highlighted.

2.1.1 Asset Container Perimeter

An asset container is the physical and/or logical location of a resource. The asset container perimeter is the first point of the container where the user encounters controls. Controls at this layer should normally be the most stringent because this is the layer closest to the asset. Figure 2-2, items 4a and 4b are two examples of common asset containers, a safe and a network-attached computer. The safe may contain a SecNet 11 network card, an administrative password list, or other controlled item. If the safe contains a hard drive with classified data, then the asset container is not the safe but rather the hard drive. The computer may contain a sensitive database or provide access to a restricted network or Enclave such as SIPRNet.

The outermost access control perimeter will be located at this level for physical assets protected by a safe or secure container. This is also the innermost access control perimeter for gaining access to logical assets through use of remote or wireless connection methods.

2.1.1.1 Physical Asset Containers

Physical asset containers such as safes, vaults and Sensitive Compartmented Information Facilities (SCIFs) are used at this layer to protect classified material and equipment. Classified materials must also be properly marked, tracked using a log, and transported using the proper cover sheets and wrapping as required by DoD policy. Security guards, automated entry biometric systems, smart cards, memory cards, badges, tokens, and other forms of access control methods can be combined at this perimeter to control and monitor access. Deterrents such as posted signage and alarms can also be used. Checklists and periodic inspections are required by DoD policy.

2.1.1.2 Logical Asset Containers

Logical asset containers include networks such as Secret Internet Protocol Router Network (SIPRNet) or Non-Classified (but Sensitive) Internet Protocol (NIPRNet) Enclaves. DoDD 8500.1 defines the Enclave as a "collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security". The security solution for the computers and networks generally includes one or more layers of physical security measures which limit access to the location and hardware of these assets. The exception is remote access (telework) which is discussed below. Securing this asset container perimeter requires access control and protection mechanisms protecting:

- Network client perimeter
- The Enclave perimeter
- The data and communications while in transit and at rest
- Server or host perimenter
- Applications (e.g., office automation, web servers, and email)
- Databases

Protection of logical assets often entails use of multiple security controls and authentication techniques as depicted in Figure 2-2. As shown, each security layer closes or mitigates security gaps but leaves no one technique can address all risks. This drawing may be viewed in conjunction with Figure 3-1 which depicts these layers in terms of technologies used in the infrastructure. Since no one technique or technology will mitigate all types of risk, use of several techniques is recommended providing these methods are chosen correctly using the methodology discussed in Section 5.

.

- Use of and adherence to administrative policies such as DoD instructions and STIGs which give guidelines for protection of logical assets;

- Integration of physical security methods such as locks, safes or SCIFs to deter unauthorized physical access to client and network devices, network rooms, ports, and cabling;

- Proper placement and configuration of architecture components such as firewalls, Intrusion Detection Systems (IDSs), ports and protocol restrictions, and Virtual Private Network authentication;

- Cryptographic logon using authentication methods such as DoD-approved PKI to ensure authenticated and authorized access;

- Use of data and communication protection mechanisms such as encryption;

- To detect unauthorized access and ensure rapid recovery of the system, implement auditing, backup, and install/update virus and malicious code protection software.

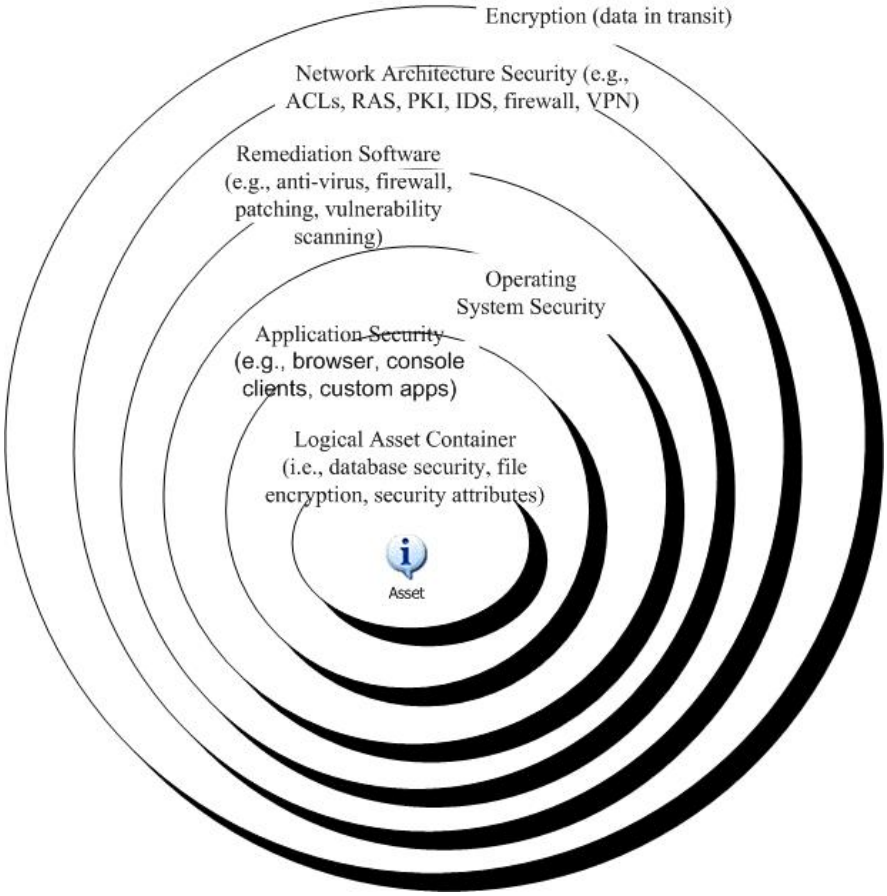

Figure 2-3. Layered Protection of Logical Asset

The primary sources for policies applicable to the logical perimeter are DoDI 8500.2 and the applicable DoD STIGs which provide implementation guidance for DoDI 8500.2 policies. These documents provide standards for protecting data at rest and in transit, user authorization, and

required administrative controls needed for protecting DoD logical assets. The primary source for policies applicable to the physical perimeter is DoD 5200.8-R.

Wireless and remote computing usually bypass the outer physical layers of the access control framework. The user enters the logical Asset Container Layer and requests access to the Enclave. In this case, the additional assurance provided by the physical layers is not present. Multi-factor access control methods, discussed in later sections of this document, must be used to support wireless and remote computing in order to achieve the desired level of assurance. Careful combination of the proper methods is particularly critical when protecting high value (i.e., sensitive or classified) assets. Further information on remote access (telework) is available in Section 3.

2.1.2 Workplace Perimeter

The workplace can be a single room, suite, or area on one or multiple floors of a building or installation. Figure 2-2, item 3 depicts one example of commonly used workplace layer, an office in a multi-story building. The workplace layer is most frequently used as the access control perimeter in DoD facilities and installations. This is because workplaces are typically smaller, defined areas that lend themselves to effective controlled access implementations. If a workplace is an open storage area which is cleared for processing for classified materials, the asset container perimeter and the workplace perimeter are the same and stringent methods must be used for perimeter controls.

To protect the workplace perimeter, the ACPs must be identified and secured. Potential access points such as elevators, stairways, windows, doors, and walls must be considered. Also consider ventilation, plumbing, electrical ductwork, and drop-tile ceilings when guarding against adversarial access. Workplaces located in a mid-level floor at least 18 to 20 feet from the ground or below roof level provide a more easily secured environment than a ground level or top floor room.

In many environments, individuals without the required need-to-know may enter a building but must remain outside of the workspace perimeter. Gardeners, maintenance contractors, and delivery people may be allowed access at the building perimeter but blocked at the workspace perimeter. In this case, the building perimeter is not part of the asset’s access control environment. A guard or attendant, who is trained to identity-proof visitors in accordance with DoD policies and subsequent sections of this document, should be used in workplaces with frequent visitors. In many cases, both automated systems and manual systems are used, where the automated systems support those who routinely work in the protected area and the receptionist or guard supports visitor access processing.

Tracking both entry and exit of authorized users should be considered to circumvent possible use of copied or fake access control credentials. This type of tracking can detect use of credentials already used for entry but not yet used for exit (i.e., the authorized individual is already within the building). Conversely, if the adversary entered first and the authorized individual was denied access, the security guard could be alerted to search for the imposter.

2.1.2.1 Secure Rooms

Unless the workspace is an approved Secure Room, classified physical assets must be in the custody of a cleared, authorized individual at all times and must be returned to the GSA-approved container or destroyed when the need for access is no longer required. All procedures for the storage of classified assets must be defined and employed in accordance with DoD 5200.1-R, Information Security Program and defined in the Target of Evaluation (TOE) Security Policy.

Secure rooms must meet the standards of Appendix 7, DoD 5200.1-R, Information Security Program and be designated in the Security Standing Operating Procedures. Any waiver to the standards set forth in 5200.1-R must be approved at the OSD level.

2.1.3 Facility/Building Perimeter

A facility is any single building, project, or site. Figure 2-2, item 2 depicts one example of a commonly used facility/building perimeter, a guarded building entryway. Note that the loading dock at the side of the building must also be secured. The facility/building perimeter may also be designated as the asset's access control perimeter. Government assets are housed in both commercial and government-owned or leased buildings. Consider the building depicted in Figure 2-2. This building has many ACPs to be considered. Main entrances and exits, emergency exits, windows, fire escapes, loading docks, roof accesses, sewer access, and connected parking garages. Often, only some of the individuals requiring access to the building or facility perimeter are authorized for access to specific assets protected within the facility. Additional identity-proofing will be required closer to the protected asset to ensure that authorization and permissions are verified before access is granted.

Security Managers should use the results of the risk assessment (as defined in later sections), to validate the need for implementing access controls at this layer in order to avoid overprotecting the asset. If the building requires frequent access by visitors, other workers in the building, maintenance staff, gardeners, delivery persons, consider the cost and complexity of implementing the required controls. If the need is valid, entry procedures for these temporary workers and also for emergency personnel are needed. If the perimeter can be established at the building layer, the level and complexity of the building internal area controls can be diminished without negatively affecting security assurance of the asset(s) being protected. On the other hand, if it is not practical to establish a perimeter at the building or facility layer, the Security Manager or Team should attempt to establish the access control perimeter as far as practical from any classified operations or assets within the building (e.g., at a controlled workspace within the building as described above).

2.1.4 Installation Perimeter

An installation is a defined base, camp, post, station, or other activity under the jurisdiction of the DoD, including any leased space. This security layer is usually not considered to be close to the asset and is usually not designated as the Asset Container Layer perimeter by the design team. When the access control perimeter is at this layer, personal authentication assurance

commensurate with the value of the assets being protected will be required at any entrance to the installation. Figure 2-2, item 1, shows that fencing may be one type of installation perimeter.

While control method at the installation layer can add to the defense of an asset, this is not always the case. Some commercial installations do not lend themselves to implementation of stringent installation perimeter controls. While Government-owned installations frequently implement multiple controls at this perimeter, commercially leased spaces such as office parks are generally open to the public. Many do not have a building guard or attendant and many cities or owners object to certain types of barriers and security controls.

The barrier is the primary means of access control at this layer. A barrier is an obstacle that prevents or controls movement of persons or vehicles. At the installation layer, the barrier is a physical security measure that prevents penetration of an installation. Barrier defenses are intended to be obvious to the potential intruder and are generally clearly marked with warning signs. Assessment and selection of a barrier solution must consider two potential penetration types: overt penetration by force and covert penetration by stealth tactics. The objective of a barrier is to physically or psychologically discourage a less determined attacker, delay a more determined attacker, and to channel the flow of personnel and vehicles.

All barriers can be compromised given enough time and resources. The objective when designing this layer is detection and delay of the attacker, giving responders enough time to neutralize the attacker. The security architect should consider the following: layering of barrier types; implementation of penetration detection systems such as alarms and sensors; and an incident response plan.

NOTE: Many of the same techniques can be used at either the Installation or the Building Perimeter.

3. ACCESS CONTROL METHODS

This section defines access control methods used in asset protection solutions and details the policies, which must be applied when implementing each technique. These solutions may be used at any layer of the security architecture and are most often used in combination (i.e., layered) to achieve the desired asset assurance level. Information on combining security technique to form a layered solution is given in Section 5 of this document.

Access control methods are specific physical or logical techniques that can be implemented at each security architectural layer to control and monitor access in and around the controlled area. There are three general types of access control methods: logical, physical, and administrative controls. Logical control methods employ hardware and software technology in various configurations and degrees of sophistication. Logical controls include firewalls, requirements for certificate-based authentication, or usernames and passwords. Physical perimeter controls form a layer of protection using interior or exterior controls to deter or delay aggressors attempting forced, visual, or even electronic access (by deterring physical proximity to the information system). Physical controls include cipher locks, physical intrusion detection systems, and guards. Administrative controls are regulations, guidelines, policies, and local procedures and are critical to the success of physical and logical control methods.

An access control perimeter is protected by one or more access control methods. The particular method used is based on variables such as the asset's value, an assessment of risk to the asset, and consideration of environmental constraints. A method having highly desirable technological capabilities may be negated by the need for constant maintenance because of the desired placement of the ACP. Some environments may cause damage to hardware (e.g., card readers or remote video systems). Conditions such as frequent sand or driving rain storms will impact the decisions made when selecting an appropriate security solution.

Methods are also evaluated based on effectiveness in mitigating likely attacks. The types of tactics against which protection is needed will differ for physical perimeters and logical perimeters. Control methods such as doors with locking mechanisms based on Personal Identification Number (PIN) entry or presentation of an identification card can be defeated given enough time, opportunity, and expertise. The adversary must be physically present to gain unauthorized physical access. If an attendant or guard is used to validate a photograph or ensure proper use of biometric systems (attended access control), then this type of vulnerability may be mitigated.

On the other hand, a successful breach of a logical access control method is not always as obvious. The adversary does not have to be physically present and may not leave physical evidence of a successful breach behind. Altering audit logs or erasing malicious code after the attack may cover the attacker's tracks, leaving the system vulnerable to continue breaches. An adversary attempting to defeat a logical data container perimeter is seeking access to data protected in an information system. In this case, an access method aimed at detecting unauthorized attacks must be integrated into the access control architecture. Thus, an access control solution must include multiple methods that work together to allow authorized users but also protect, deter, and detect unauthorized attacks.

3.1 Identification Credentials

Identification is the process by which information about a person is gathered and used to provide some level of assurance that the person is who they claim to be. The identification process results in the issuance of a credential. A credential is something that an entity (user or device) provides to validate a claim of identity. The credential may be something given to the person, that can be presented to the system (e.g., an ID card or password) or it may be created by the user during the authentication process (e.g., a digital signature). However, not all credentials are equal. The level of assurance provided by a credential depends on that of the underlying identification process and the credential type. Once issued, the credential must be validated as part of the authentication process which is discussed the following subsection. Obtaining access to a controlled asset requires the user to assert an identity and then provide a credential as proof of that identity. (However, the individual must also have authorization to access the asset, regardless of the validity of the identity. Authorization is discussed in a subsequent section).

Before receiving credentials, an applicant must demonstrate that the identity claimed is real, and that this is the entity (e.g., person or server) that is entitled to use that identity. DoD policies includes processes for identity-proofing and issuance of identity credentials. Organizations in DoD use the CAC, photo badges, digital signature, or username/password pairs as credentials. Credential issuance generally involves the following steps.

- Identity-proofing, where the claimed identity of the entity is validated. In DoD, this requires background checks and other means of verifying documents, biometric comparisons to criminal history database, and other information provided by the claimant. Security managers will verify identity using an ID card (s) issued through an appropriately rigorous process prior to issuing local credentials. Where multiple proofs of identity are required, care should be taken to require use of ID cards issued using different identity proofing processes.

- Registration and naming, where the entity is assigned an identifier

- Generation of an authentication credential. Depending on technology used, may involve selection or generation of PINs, PKI certificates, photograph, and/or biometric reference samples.

- Binding the intended authentication method to the identity.

DoD Directive 8190.3, *Smart Card Technology*, identifies the CAC as the "standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals". The Directive states that the CAC will be the principal card used to enable physical access to buildings, installations, and controlled spaces. However, the policy does not require use of CAC and local managers can not require CAC for personnel who are not eligible for the CAC. While this directive does not preclude the use of locally issued identity cards, including a verification of the CAC as part of the local credential issuance process will take advantage of the robust CAC identity proofing process whenever possible; thereby add to the assurance level of the locally issued credential.

- *(AC31.010: CAT II) Before granting access to non-public information systems (e.g., Privacy Act, FOUO, classified), the IAM, will ensure all personnel are properly identified according to applicable DoD policy (as required for level of access and information sensitivity).*

- *(AC31.020: CAT II) The Security Manager and IAM will ensure authorized users are trained to exercise care in the protection of their identity credentials (e.g, CAC, visitor badges).*

- *(AC31.030: CAT III) The IAM will ensure DoD-approved PKI is used to authenticate logical access to Information Technology systems and applications that access the Department's computer networks. If certificate-based authentication is not used, a documented migration plan is required. The DoDI 8520.2 policy provides for exceptions for systems that have communities not eligible to be issued PKI (e.g., dependants, retirees).*

- *(AC31.035: CAT III) The Security Manager and IAM will ensure compliance with the following out processing requirements:*

  – *V0007210: A program exists to ensure personnel out process through the security section. (Traditional Security Checklist).*

NOTE: Includes turning in of all access badges, classified or sensitive information and signing of SF 312 acknowledging debriefing. Also, revoking and reporting of electronic credentials in accordance with DoD policy for the DoD CAC, DoD-approved PKI, and disable system accounts. User's CAC is not captured unless the person is leaving DoD.

- *(AC31.045: CAT II) The Security Manager will ensure badges and credentials for Foreign Nationals comply with the following:*

  – *V0007163: Ensure foreign visit requests is processed through DIA and then referred to the DISA Security Division (MPS6). (Traditional Security Checklist)*

  – *V0007138: A contact officer is appointed to control the activities of foreign visitors, FLO, and exchange personnel (Traditional Security Checklist)*

  – *V0007135: Foreign nationals assigned to the command are issued badges or passes that clearly identify them as foreign nationals. Proper guidelines are being followed when the badges or passes are issued. (Traditional Security Checklist)*

- *(AC31.050: CAT I) The Security Manager will ensure authorized personnel validate the identity of any person prior to issuing an authentication token (such as an unescorted visitor's badge, a CAC or local identity credential) to that person.*

3.2 Personal Authentication

When an individual presents an identity credential at a logical or physical access control point, the credentials must be authenticated as valid and bound to the claimant. Credentials are authenticated using one of three personal authentication factors or techniques. The three categories of authentication factors are:

- *something you know* (e.g., a password),
- *something you have* (e.g., a certificate with associated private key or smart card), and
- *something you are* (a biometric).

Single-factor authentication is defined as the use of any one of these categories or authentication factors. If two factors are employed, this is considered two-factor authentication. Finally, if all three factors are required then this constitutes use of three-factor authentication. Individual authentication assurance increases when you combine authentication technologies and techniques, especially when combining differing authentication factors.

The access control process includes the following:

- Assessing access privileges based on validated identity and need-to-know.

- Allowing or denying access privileges based on mapping the identity contained in/on a validated credential to privileged or system configuration information (i.e., access control lists, privilege token databases, or policies).

The level of assurance provided by a personal authentication method such as a smart card, key, or token, is increased as the number and types of authentication factors are increased. Because classified and mission critical assets require greater levels of authentication assurance than For Official Use Only (FOUO) assets. There is currently not a clear requirement for three-factor authentication for classified assets but authentication methods giving a higher level of assurance should be used to protect these information assets. The table in Section 5 will assist the security manager in choosing valid combinations, which will provide the desired level of protection based on the value of the asset being protected. The table illustrates how the concept of something you have, something you know, and something you are can be leveraged to optimize the access control architecture.

- *(AC32.010: CAT I) For information systems processing sensitive information, the IAO will authenticate identity credentials using multi-factor authentication prior to allowing access..*

3.3 Authorization

The *Compliance and Review of Logical Access Control in the Department of Defense (DoD) Processes* Memorandum dated 24 January 2007 addresses the need to access control measures private web servers, web-based systems and applications, and web portals. DoD-approved PKI provides certificate-based authentication for all persons authorized access to log on to the network. However, this does not replace the need for mandatory/discretionary access control. Successful authentication must not automatically give an entity access to an asset or security

boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. An entity may be an individual user or an information system such as an application, operating system process, or workstation. To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems, including networks, web servers, and web portals, must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access.

The decision to grant or deny access to an asset is the responsibility of the asset owner. This decision must be based on an assessment of the entity's need for access to the protected asset. This need should minimally involve the identification of clearance level requirements (based on the required Confidentiality Level of the asset) and an assessment of whether access is needed for conducting official duties. Once criteria for authorization are established by the data owner, this information is passed to all entities responsible for configuration or enforcement of access control such as system administrators or attendants.

Once an entity has been identified and authenticated, authorization is performed at the asset container perimeter. Authorization for both physical and logical assets can be implemented as a combination of manual, automated, and/or administrative methods. Authorization methods include access control lists or validation of a security attribute. Logical or physical access control lists may be used to record rights and permissions. Organizational procedures must be established to ensure these lists are updated when these rights are revoked. This list can be a log used by an attendant or implemented using technology such as in an automated entry system or other information system. A security attribute is a security-related quality of an object. Compartments, caveats, and release markings are attributes that are assigned to DoD entities based as dictated by established security policies. Security attributes can also be determined manually but are increasingly electronically bound to an entities identity token.

For information systems, the authorization process may be used to produce a security token that is only valid for the duration of the current authenticated session. The token binds the user's privileges, group membership, and other security attributes to the identity. The system then uses this security token to control access to objects and the ability of the entity to perform various system-related operations on the client or network. The token can also be passed using secure communications to trusted applications or networks for access to various resources.

According to DODI 8500.2, need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls (DAC or RBAC). Access must be based on a comparison between the user's trust level or clearance and the sensitivity designation of the information (mandatory access control). Additionally, access control systems must allow the asset owner to specify explicitly the types of access each entity has to the protected asset (DAC). In applications or databases using role-based access control, users gain access based on assigned roles. Roles are defined within the system based on job functions within the organization with regards to the authority and responsibilities of the users assigned to each role. RBAC can reduce the complexity and cost of security administration in large networked applications. However, this type of access control must be implemented effectively using properly applied permissions,

administrative procedures and review when establishing and maintaining roles, and the available functionality of the system should be carefully evaluated prior to procurement. DoD policy and each applicable STIG, requires that all privileged user accounts are established and administered using role-based access control that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration) and that privileged role assignments and access be tracked and audited.

A deny-by-default policy, where access to physical or logical assets is denied unless explicitly permitted is mandated by DoD policy. When designing or implementing access control procedures or systems, system/application owners and system administrators shall comply with the following policies as well as the policies of the Enclave and Application STIGs.

- *(AC33.010: CAT II) Before granting access to sensitive, restricted information, the IAM will ensure users have a demonstrated need-to-know as determined by the data owner. Access is granted in accordance with clearance levels, IT level and DoD 5200.2-R.*

- *(AC33.015: CAT III) The IAO or Security Manager, in coordination with the data owner, will document rules for who is authorized to access the system. Access rules allow the system or attendant to determine who or why access is needed (e.g., allow all DoD employees; all members of a specific community of interest; all entities that are assigned to a specific role; or by physical or logical access control list.*

- *(AC33.020: CAT II) When applicable, ensure mechanisms are in place to allow appropriate users to access information that has been cleared for release to the represented foreign nation, coalition, or international organization in accordance with related policy (e.g., DoDD 5230.11, DoDD 5230.20, DoDI 5230.27).*

- *(AC33.025: CAT I) The Security Manager or IAM will ensure a program exists to ensure personnel out process through the security section.) (Traditional Security Checklist).*

NOTE: This includes that mechanisms are in place to verify individuals are still authorized access to information systems and permissions have not been revoked. A rules-based process will be established for determining how personnel are authorized, for linking personal certificate information to authorization(s), and for removing authorizations when access is no longer needed.

3.4 Logical Access Control Methods

This section discusses technologies and techniques which are authorized for use within DoD to support the validation of the digital identity of an individual. Although there are many commercially available products, only technologies that can be employed in a manner meeting the requirements of DoD policies are included.

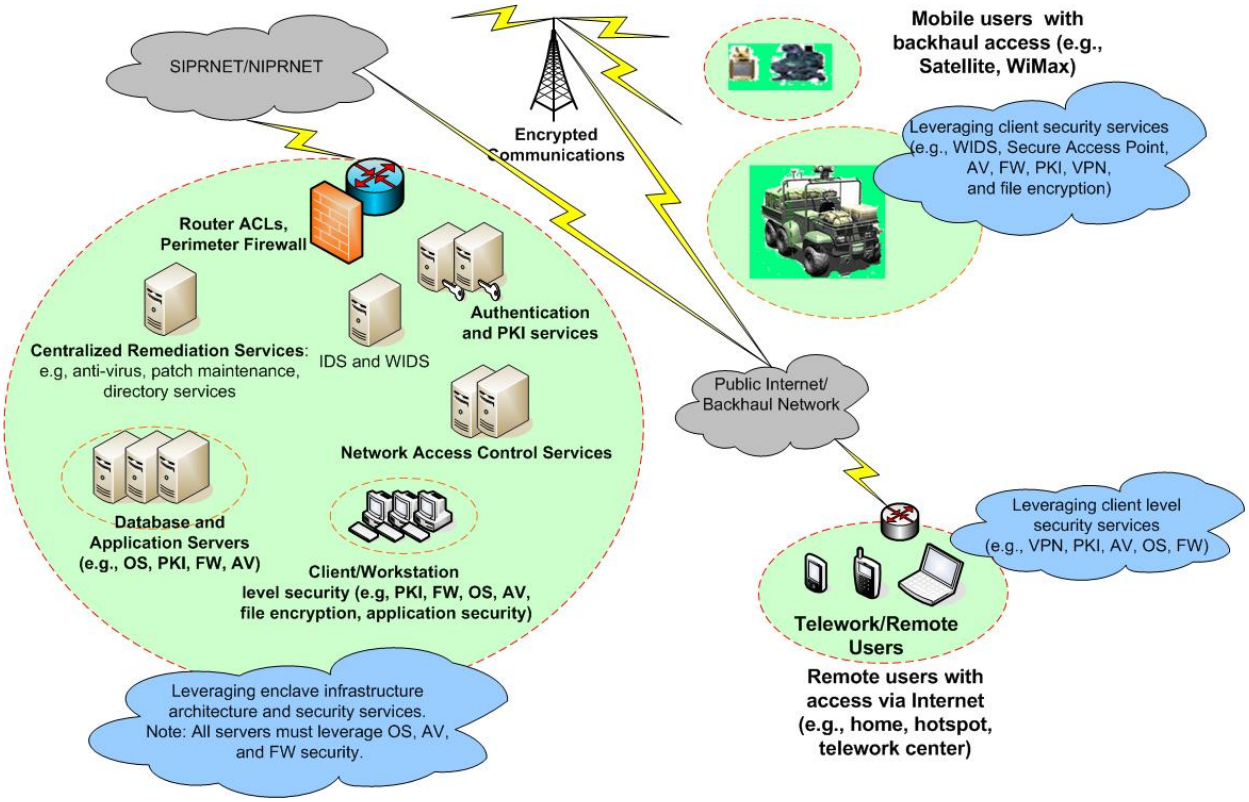

Figure 3-1. Example of Leveraging of Logical Security Sevices

- *(AC34.010: CAT III) The IAM will ensure newly purchased information systems intended for use as or integration into access control solutions which protect DoD information assets are evaluated using the required evaluation processes.*
  - *GOTS products are evaluated either by NSA or using an NSA-approved process (e.g., using the applicable FIPS publication and STIG).*
  - *COTS products are evaluated through one of the following sources:*
  - *The International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement;*
  - *The NIAP Evaluation and Validation Program; or*
  - *The FIPS validation program.*

Historically, username and password combinations have provided identification and authentication for access to networks, clients, and automated access control systems. With the advent of new technology, additional logical access control methods provide improved assurance, particularly when combined to result in multi-factor authentication resulting in the current DoD mandate to minimize use of password access and require PKI based authentication for most systems. Logical and physical control methods can be combined or interchanged to

give equivalent assurance depending on the environment and technical requirements of the data owner and organization. Logical security services, architecture, and technology are always based on a risk assessment of existing technological solutions. As changes in programming techniques (data elements and relationships); communication models (e.g., peer-to-peer, distributed); and attack methods occur, the security assumptions and design must change to manage the resultant threats.

3.4.1 Techniques for Security Network Access

Network access control techniques work together to stop unauthorized access, prevent malicious endpoint activity, and enforce your organization's security policies. The following sections describe various physical and logical methods for security network access.

3.4.1.1 Network Architecture Controls

DoD policy requires use of logical access control mechanisms to protect the Enclave. These mechanisms are extensively described in the Enclave and Network Infrastructure STIGS and are not repeated in this STIG. Sites implanting these network infrastructures should comply with the access control implementation policies in the appropriate STIGs. These mechanisms include:

- Remote Access Servers: A Remote Access Server (RAS) or Network Access Server (NAS) serves as the access control point to the Enclave perimeter. NAS provides all the services that are normally available to a locally connected user (e.g., file and printer sharing, database and web server access, etc.). Permission to dial into the local network is controlled by the NAS and can be granted to single users, groups, or all users. NAS and RAS devices can also interface with authentication servers.

- Authentication Servers: Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access System (TACACS) provide access and authentication for remote users.

- Access control lists (ACL): Include restrictions on inbound and outbound connections, as well as connections between LAN segments internal to the site/enclave.

- Firewalls: Controls the traffic flow between a trusted network and an untrusted network. Usually firewalls are used to protect the boundaries of a network.

- Logical IDS: Network and workstation mechanisms that monitors network traffic and provide real-time alarms for network-based attacks Service Network.

- De-militarized Zones (DMZ): A perimeter network segment that enforces the internal networks information assurance policy for external information exchange.

- Audit Log and Log Analysis: network, server, and application logging is required to protect DoD restricted information. On large networks, this service is usually centralized to a logging server although some devices or applications cannot support this capability and must log on the device. Devices without any auditing capability should not be used

in the DoD Enclave. Minimum requirements for activity logs depend on the type of device or application and are available in applicable operating system STIGs. While logging itself is automated, log analysis can be automated and/or manual. A sound best practice, particularly for critical systems, is that someone other than the system administrator should perform log analysis. Personnel with access to system logs should be specifically designated and assigned permissions accordingly. The Security Manager, IAM, or designated personnel will review system activity logs regularly looking for trends and anomalies which can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network.

- *(AC34.015: CAT II) The IAO will ensure the Enclave architecture and components are in compliance with the Enclave and the Network Infrastructure STIGs.*

NOTE: Comply with this requirement by conducting self-assessments or Security Readiness Reviews using the applicable STIG security checklists that apply to the various technologies used as part of the Enclave architecture.

3.4.1.2 Remote Network Access

Remote access (telework) to sensitive and classified information must employ stringent security for the communications and for the client device. Classified remote access will require use of an NSA approved Type 1 device. Remote administrative access requires the use of encryption to protect the communication. With the use of digital certificates, strong authentication mechanisms are more readily added to the remote access solution and must also be used prior to allowing the remote access.

For remote access, security configuration typically involves use of a VPN tunnel, including use of required encryption and authentication of the remote client prior to granting access. The network architecture and client configuration settings for a PPP network are discussed in the Secure Remote Computing, Desktop Applications, and the Network Infrastructure STIGs.

- *(AC44.010: CAT I) The IAO will ensure NSA approved, Type 1 device is used to protect remote access to classified networks.*

- *(AC44.015: CAT I) The IAO will ensure remote administration of network devices, servers, and applications are protected by NIST FIPS 140-2 validated cryptography to implement encryption for communication.*

- *(AC44.020: CAT I) Remote access to NIPRNet and SIPRNet resources must be approved by the DAA and must comply with NSA and DoD policies and guidelines.*

- *(AC44.025: CAT I) The IAO/NSO will ensure an NSA approved remote access security solution (such as a HARA solution) is used for remote access to a classified network.*

- *(AC44.030: CAT II) The IAO will ensure remote access configuration and user training is compliant with the Secure Remote Computing STIG.*

3.4.1.3 Securing Network Ports

Network ports should be both physically and logically secured to prevent unauthorized access to the DoD Enclave. The assurance level of the physical security method implemented should be consistent with the policies for the sensitivity and mission critically of the network. These security measures are particularly critical when considering SIPRNet and wireless access controls. When a computer is physically connected to a network port manual procedures and/or an automated method must exist to perform the following security functions:

- Verify the computer is authorized access;
- Verify that the user is authorized access; and
- Verify that the computer configuration is compliant with security standards.

The following sections discuss various methods used in DoD for security network ports both physically and logically.

3.4.1.3.1 Physical Security for SIPRNeT Ports

Network ports with access to SIPRNet must be both physically and logically secured. SIPRNeT network ports must be physically protected at the Secret level using one of the following techniques:

- A Hoffman Box and MAC address filtering or

- 802.1X authentication implemented as follows:

  - Drop may terminate in a room that meets Open Storage requirements and has been approved for that use.

  - The end of the cable, leaving the PDS Conduit or wall (in a Secret CCA), must be secured in a lock box. The lock box has to be a significant metal box, no other punch out slots, the conduit going in has to be welded or epoxied, the hinge needs to be inside, welded or pinned, and the hasp should be heavy and inside. Hoffman Boxes are built for that purpose and exceed any requirements. It must be secured with a 3-position GSA approved lock, which currently is the Sergeant & Greenleaf. A high security key lock may be used, but the key must be stored in a GSA approved safe or vault. However, the high security key lock does not fit the Hoffman box due to the shackle size.

  - While having Open Storage or a lock box is preferred, as an alternative, the classified circuit may be disabled during non-duty hours at its origination point.

  - The use of 802.1X has been approved by the SCAO for protection of SIPRNet ports. It has been included in the Network STIG as an option for port security. This is the only current port security solution and must be fully implemented. The use of

802.1X does not remove or mitigate the requirement for a PDS. 802.1X compliance requirements are discussed in a subsequent section.

NOTE: Additional information and policy requirements for physical protection of SIPRNet port can be found in the DISA Traditional Checklist.

3.4.1.3.2 Logical Network Port Security

Both unclassified and classified networks require the implementation of a logical network port security solution. Network devices can be used to implement electronic locking of network ports. This method is commonly implemented by configuring the network switch such that specific ports accept connections from one or more specific MAC address (es). Only a device configured with the authorized MAC address is allowed to access that network port. The port must be configured so that if an authorized device is unpluged the port becomes locked, preventing "piggybacking" of an unauthorized user. Port security is particularly important for ports installed in locations such as conference rooms, hospital rooms, lobbies, or other uncontrolled areas. However, there are a few issues with MAC address based authentication and authorization security that must be considered.

First, since MAC addresses are easily spoofed, an intruder could use a device configured with a previously authorized MAC address to gain access to the network. An intruder today can easily alter the MAC address of another device, unplug the "safe" device and insert the alternate MAC device, thus gaining access to the network. Additionally, end-point devices exist on the network today that may never be able to run an advanced network stack containing authentication options for the device (e.g., IP Phones, medical scanners, various sensor devices). Often these devices are critical requirements for the mission but will not be able to conform to port security or port authentication requirements. Finally, on a large network, there is a significant administrative overhead associated with the creation and maintenance of per port MAC address controls.

In these cases, port security alone does not provide enough assurance to deny an intruder access to the network based on only MAC address authorization. Additionally, a layered solution that combines several access control techniques will best provide the required level of assurance. Minimum acceptable requirements for network access security are as follows:

- MAC Address Authorization configured for to protected each network port;
- MAC Address Profiling (e.g., medical devices, logistics scanners, sensors, etc); and
- Secured VLAN deployment for devices that meet this standard and can not meet more intelligent solutions such as security posture assessment.

A secured VLAN is commonly created for groups of devices that are less trustworthy based on the overall security posture of the device. Within the context of this network (VLAN), all egress activity to the normal network is controlled via a firewall, Intrusion Prevention System (IPS), or other network monitoring device. This ensures that devices that could be MAC spoofed and have not passed further policy inspection because of device capabilities can be more closely scrutinized prior to gaining access to the network. Furthermore, unused ports on the network

should be disabled until needed. Further, if Virtual Local Area Networks (VLANs) are used on a network, a good security practice is to place disabled ports in a separate VLAN.

By employing more advanced network access control technology, the network security posture is significantly improved over relying only on a MAC address lock mechanism. MAC profiling and Address List Authorization allow devices to be moved within the network without tying a single device to a single location, but providing a "master list" of approved devices. This greatly decreases the administrative burden associated with per port MAC Security and increases network flexibility while maintaining a higher level of security posture for the network over relying solely on per port address locks.

- *(AC34.020: CAT III) The IAO/NSO will ensure disabled ports are placed in an unused VLAN.*

- *(AC34.025: CAT I) The IAO/NSO will ensure either MAC security (with profiling) or 802.1X port authentication is used on all network access ports and configured in accordance with the Network Infrastructure STIG.*

- *(AC34.030: CAT III) The IAO/NSO will ensure if logical Port Security is implemented using MAC filtering, then the MAC addresses are statically configured on all access ports.*

3.4.1.3.3 Port Authentication Using 802.1X

The 802.1X protocol is an authentication standard that can be used for wired or wireless networks. This standard provides for user/device authentication as well as distribution and management of encryption keys. Individual client sessions use different keys and keys are changed dynamically. As shown in figure 3.2, there are three components that are used to create an authentication mechanism based on 802.1X standards: the client/supplicant, the authenticator, and the authentication server.

- Client/Supplicant: The client, or supplicant, is the device that needs authenticating to the network. It supplies the username and password information to the authenticator. The client uses the EAP to talk to the authenticator.

- Authenticator: The authenticator is the device performing the 802.1X port authentication to control access to the network (this is most likely an 802.1X switch). The authenticator receives the username and password information from the client, passes it onto the authentication server, and performs the necessary block or permit action based on the results from the authentication server. The authenticator uses RADIUS to speak to the authentication server.

- Authentication Server: The authentication server (e.g. RADIUS) validates the username and password information from the Client and specifies whether or not access is granted. The authentication server can also be configured to specify authorization by assigning the device or port to a VLAN access.

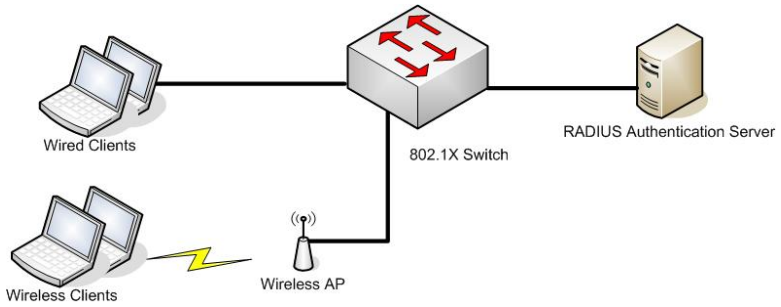

Figure 3-2. Example 802.1X Implementation

802.1X clients use the EAP and EAP Over LAN (EAPOL) to secure communications between the client and authenticator. Before the client is authenticated, the network port is set to the unauthorized state and only allows EAPOL authentication traffic between the client and the authentication server. All other normal data traffic is blocked. When the client authentication is complete and access is granted, the controlled port is set in the authorized state and is granted network access. To authenticate a client, the authentication proxy will compare the username and password entered by the client to the user identification and password parameters in the authentication directory (e.g., Microsoft Active Directory). Once the client/user is authenticated successfully, proper authorizations must then be associated with the user.

Wireless port access is a particularly vulnerable area where port security solutions are critical. Use of 802.1X authentication has been made mandatory by the 802.11i WLAN security standard, thus products meeting the WPAv2 requirements will be compatible with enterprise level 802.11i authentication servers, such as the Remote Access Dial-in User Service (RADIUS) server. The RADIUS server can then pass off the backend authentication to enterprise authentication services provide directory services such as Microsoft Active Directory.

The use of 802.11i configured to use AES encryption, 802.1X authentication services along with the EAP provides the best solution for the enterprise level network, particularly a high security environment. Additionally, 802.1X can be used to provide a layer of protection from unauthorized wireless access points on the wired network, as all devices are required to provide authentication credentials to the network switch port prior to obtaining access. However, the protocol must be configured securely and implemented as part of a layered security solution, in conjunction with other security measures such as IPSec, VLAN assignments, user authentication, and with host/client level security.

- *(AC34.035: CAT II) The IAO/NSO will ensure directory authentication services (e.g., Active Directory) use PKI or encrypted passwords for administrative access on production systems.*

- *(AC34.040: CAT II) The IAO/NSO will ensure when utilizing 802.1X, a secure EAP method (e.g., EAP-TLS or EAP-TTLS) resides on the authentication server and within the operating system or application software on the client devices.*

- *(AC34.041: CAT III) The IAO/NSO will ensure 802.1X port security violations are sent to an audit log.*

- *(AC34.045: CAT I) The IAO/NSO will ensure if 802.1X Port Authentication is implemented, all access ports start in the unauthorized state*

- *(AC34.050: CAT II) The IAO/NSO will ensure if 802.1X Port Authentication is implemented, re-authentication occurs every 60 minutes.*

802.1X port security can either be configured for multi-host or single-host mode. The required configuration is for single-host mode. In this mode if the port detects a second machine connected to a port in the AUTHORIZED state, that port is immediately transitioned to the UNAUTHORIZED state and can no longer be used for network access. This security feature detects and prevents unauthorized connection of a hub or switch after an authentication session has been initiated. An attacker could disconnect the authorized computer, connect a switch to the port, and reconnect both the authorized and unauthorized computer to the port. A similar exploit could be implemented using a wireless access point. This exploit is one reason why a layered security is needed when implementing 802.1X.

- *(AC34.051: CAT II) The IAO/NSO will ensure if Port Authentication is implemented, all access ports are configured in single-host mode.*

3.4.1.4 Network Access Control (NAC) Systems

NAC Systems enforce network security policy at the network access point rather than the client (endpoint) operating system. Depending on the system architecture and configuration, NAC systems can provide physical port security or logical port/access security. NAC systems require authentication for both the endpoint and user before the network access point forwards traffic for that client. NAC systems also require authorization of the client operating system security posture before being allowed access to resources on the network. Endpoints or users that fail authentication are blocked from any network access either by physically shutting down the port or logically by blocking the MAC or IP address, depending on the deployment scenario. Client devices or users that fail security policy authorization are “quarantined” into a highly restricted network area logically using restricted VLANs or ACLs and are granted just enough access to remediate the client. Once the NAC system successfully authenticates and authorizes a client device and user, the NAC system is responsible for granting the user complete or partial access to the network depending on the privileges assigned to the endpoint or user. Additional information and security requirements for this section are being developed and are planned for a future DISA STIG.

- *(AC34.031: CAT III) The IAO/NSO will ensure if NAC is implemented it is in accordance with the minimum standards set below.*
  - *All ports are placed into an untrusted state not within the normal forwarding path*
  - *Authentication is required for port to be placed within normal forwarding path*
  - *MAC Address Authorization must also be enabled for network devices not capable of performing authentication*

3.4.2 Cryptography

An integrated access control solution must allow both authorized and prevent unauthorized access. Although cryptography (methods of hiding the meaning or existence of a message) may not be considered an access control method, it is incorporated into many access control techniques and protocols. Cryptography is used for PKI certificate-based authentication and to protect the transmission of the password in username password authentication. Attacks against modern cryptography may range from analyzing the level of power drawn to help in the guessing of keys to even more advanced approaches using lasers to induce and disrupt electrical currents. To guard against attack, DoD requirements must be followed.

Cryptographic algorithms use either a single symmetric key or two asymmetric keys. In symmetric cryptography, a single secret key is used by two entities to perform the encryption and decryption process. The single key must remain secret so the encryption will be secure since anyone with the key can decrypt the message. This presents a limitation if a private secure channel for transmitting the shared key is not possible since the key may be compromised in transit. Non-repudiation is not possible in symmetric cryptographic schemes.

On the other hand, public key or asymmetric cryptography uses a pair of simultaneously generated keys to perform encryption and decryption. Because it is computationally infeasible for an attacker to use the public key to generate the private key, the public key can be sent over non-secure channels. The private key must be kept confidential, and is often stored on a separate hardware token requiring a password to activate. If the public key is used to encrypt, only the holder of the private key can decrypt the information. Conversely, if the private key is used to encrypt, the public key can be used to decrypt and verify that the sender holds the private key. This process is used for authentication or digital signature, and supports non-repudiation.

Asymmetric keys are not typically used to encrypt large amounts of data because the ciphers are slow and processing intensive. This is why public key encryption, uses an asymmetric key to encrypt the keys but a symmetric cipher to encrypt the data, particularly when the data is a large amount. Thus, public key and symmetric key encryption are often implemented together. The information to be exchanged is first encrypted with a newly generated symmetric key. Then the symmetric key is encrypted with the public key(s) of the intended recipient(s) and attached to the encrypted information.

Cryptographic-based security systems are used in various information system hardware and software applications. These products use cryptographic modules to provide security functions

such as a cryptographic algorithms, cryptographic key management, and authentication. The cryptographic module of an information system must provide a level of security appropriate for the security risk and confidentiality requirements of asset. Use of products with NIST validated cryptographic modules (unclassified systems) or that are NSA approved, Type 1 products (classified systems) provides assurance that the cryptographic mechanisms used is compliant with DoD standards and techniques. These standards specify the security requirements that will be satisfied by a cryptographic module used within a security system protecting sensitive information.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules using the Federal Information Processing Standard (FIPS) 140-2 (FIPS 140-3 is currently in draft) and other cryptography based standards. Products validated under the CMVP are accepted by Federal agencies for the protection of sensitive information. The FIPS 140-series of standards provide assurance that a validated module is used but the cryptographic process must also use only NIST approved algorithms such as AES or 3DES. These standards specify technical requirements for certifying cryptographic software and hardware modules. Certified cryptographic software and hardware modules must meet one or more of four security levels of compliance under FIPS 140-series standards using approved algorithms and the required modes for those algorithms; meet requirements for key management and power-up tests; and have applicable documentation. Modules for certification are evaluated by one of 14 laboratories in the United States, Canada, the Germany, and the United Kingdom.

The FIPS 140-3 revision is expected to be published by the end of 2007, however, modules validated under the previous FIPS 140-1 and FIPS 140-2 standards will still be authorized for use. Changes in FIPS 140-3 are intended to keep the standard current with modern cryptographic attacks. These include a new a redefinition of the security levels and an addition of a new Security Level 5. Also, included are a clarification of key management procedures, relaxed power-up test requirements to support embedded devices, a new section devoted to software modules, and a new physical protection section.

A list of products with FIPS 140-1/2/3 validated or pre-validation cryptographic modules is available at the NIST website, http://csrc.nist.gov/cryptval/. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated using the FIPS 140-1/2/3 standards.

Although a product may use a cryptographic module and algorithms that meet NIST or NSA standards, the product must also be operated in compliance with the required configuration to achieve the desired assurance level. Review the vendor's documented cryptographic module security policy to determine if all operating system, physical security, or other security rules are required to ensure that the cryptographic module, as implemented by the site or organization satisfies the security requirements of FIPS standard. These required security policies may also incorporate or specify the need for added access control and I&A policy specifications.

3.4.2.1 Encryption

Encryption is the use of a cipher, algorithm, or process to transform information into a form that is unreadable without the proper decryption process and keys. Encryption cannot be used as the

only form of protection since the data inside the encryption package can still be invalid (lack of integrity) or from an unauthorized source (lack of authenticity). The communication can also be intercepted for purposes of traffic analysis which may provide the potential attacker with an essential piece of information. However, encryption is invaluable tool when used to protect the confidentiality of communications in one of two ways.

- End-to-end encryption – The data or message is encrypted from the sender to the receiver. Protocols such as Secure Multipurpose Internet Mail Extensions (S/MIME) and Secure Socket Layer (SSL) are examples of this technique. S/MIME provides end-to-end e-mail encryption when used in conjunction with DoD-approved PKI.

- Virtual Private Networks (VPN) – A private data network that maintains confidentiality through use of encryption and security procedures across a shared public telecommunications infrastructure. The data is transported or tunneled across a public or private network employing encryption technologies such as Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to Point Tunneling Protocol (PPTP). Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions.

Encryption can also be used to protect the data stored on the hard drive of the client system. Some products perform encryption and decryption transparently as the user stores and retrieves files onto fixed or removable storage media. This type of encryption is used to protect information on mobile devices such as laptops, which are more susceptible to theft. When using file encryption, ensure that the temporary and paging files version of protected files are secured. These files should not be stored in plain text and must be removed when no longer needed.

Use of encryption is required when sensitive unclassified or classified information is transmitted over an untrusted public network domain (e.g., the Internet). Encryption does not adequately mitigate threats to data integrity or authenticity, nor does it provide non-repudiation. Threats from viruses and denial of service attacks are still possible. Therefore, encryption methods must be paired with access and authorization systems that define which applications, systems, or data an entity can access.

- *(AC34.055: CAT II) The IAO/NSO will ensure communication for privileged access (i.e., administrative access) to network devices is secured using products with FIPS 140-2 validated cryptographic module and configured in accordance with the Network Infrastructure STIG.*

- *(AC34.060: CAT II) For sensitive but unclassified information systems, the remote user will use a FIPS 140-2 validated cryptographic module configured to use NIST approved encryption algorithm to encrypt sensitive government files, folders and/or storage devices on remote or mobile client devices.*

- *(AC34.065: CAT II) For sensitive but unclassified information systems, the IAM will ensure a FIPS 140-2 validated cryptographic module configured to use a NIST approved file encryption algorithm is used to protect DoD sensitive data in transit over non-DoD networks or when transmitted wirelessly.*

- *(AC34.066: CAT I) For classified information systems, the IAM will ensure use of an NSA approved, Type 1 device to implement cryptographic services.*

- *(AC34.067: CAT II) The IAM will ensure cryptographic-based security systems are implemented in accordance with the vendor-specified security policies required to ensure the cryptographic module, as implemented by the site or organization, satisfies the security requirements of the FIPS or NSA standard/requirements (i.e., configuration of operating system, physical security, or other security rules)*

3.4.2.2 PKI Compliance Requirements

PKI refers to a framework of programs, data standards, communication protocols, policies, and cryptographic mechanisms. Use of a DoD-approved PKI certificate represents two-factor authentication, *something you have* (private key) and *something you know* (PIN). Storing the PKI on a hardware token, while still an instance of two-factor authentication, results in an increased level of assurance because it increases the difficulty of a successful attack. The hardware token represents a second instance of *something you have*.

The PKI infrastructure provides for the generation, production, distribution, control, accounting and destruction of public key certificates. PKI provides a variety of services including issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates using Certificate Revocation Lists (CRLs); and related services and support. Components of a PKI include system components such as one or more Certification Authorities (Cas) and a certificate repository; documentation including a Certificate Policy document and one or more Certification Practice Statements; and trained personnel performing trusted roles to operate and maintain the system. PKI integrates digital certificates, public-key cryptography, and Certification Authorities into an enterprise-wide network security architecture. PKI provides the capabilities of digital signatures and encryption which are used in DoD to implement the following security services:

- Identification and authentication through digital signature of a challenge;
- Data integrity through digital signature of the information;
- confidentiality through encryption; and
- Assists with technical nonrepudiation through digital signatures.

One of the most important components of PKI is the X.509 formatted public key certificate. This certificate is a data file that binds the identity of an entity to a public key. The data file contains a collection of data elements that together allow for unique authentication of the owning entity when used in combination with the associated private key. These data elements include: the name of the entity or subscriber; the validity period start and end dates; the public key; the name of the issuing CA; and the digital signature of the CA.

DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" identifies requirements for the use of PKI by the DoD, including the use of approved external PKIs. DoD plans wide use of digital certificates for server authentication and strong user authentication in both wired and wireless networks (e.g. on wireless local area network using 802.1X with EAP-TLS). The DoD-approved Cas issue certificates for use by entities accessing either the NIPRNet or the SIPRNet. These certificates are issued to both software and hardware tokens. The primary token for individuals within the DoD on the NIPRNet is the CAC but other authorized tokens can be used. Additional information on PKI and PK-Enabling can be found on the PKI website, http://iase.disa.mil/pki, and the PK-Enabling website, https://gesportal.dod.mil/sites/dodpke (certificate required).

The DoD CAC is the primary hardware token for certificates issued by the DoD PKI. The CAC contains the cardholder's certificates and private keys. Identity and signature keys are generated on the CAC and never leave the CAC. Encryption keys are generated by the PKI and securely transferred onto the CAC. External PKIs including the External Certification Authority (ECA) PKI may be approved for use by DoD information systems, but these PKIs will use either software for key storage or their own hardware tokens, not the CAC. Access to private keys either on the CAC, a different hardware token, or in software requires a user provided PIN or password. The digital certificate is publicly available, thus the purpose of the PIN is to protect access to the private key rather than the certificate. As a result, the use of PKI represents two-factor authentication (the private key is *something you have* and the PIN/password is *something you know*). Using digital certificates and private keys, users can authenticate to networks or web servers, digitally sign electronic documents such as email, and encrypt/decrypt information.

DoD policy requires the use of DoD-approved PKI certificate based authentication for logical access to non-public DoD computer networks, systems, and web-based applications. JTF-GNO PKI acceleration directives require that users initially logon to the NIPRNet using certificates issued by DoD PKI. Applications should be PK-Enabled to require authentication with certificates issued by DoD-approved PKIs. Applications that have users who are not eligible for CACs must be PK-Enabled to authenticate certificates issued by external DoD-approved PKIs. Applications that have not yet been PK-Enabled must require a DoD compliant username/password combination after initial NIPRNet logon. However, it is important to note that not all users of web based applications log onto the NIPRNet before accessing the application. Furthermore, Email systems must support digital signature and encryption so users may implement theses services as and when their mission requires. Although not currently mandated by DoD policy, information systems and applications other than email that incorporate the use of PKI for digital signatures must use DoD-approved PKI and follow Department-wide interoperability guidelines for digital signature solutions SIPRNet PKI, while available, is not yet widely employed.

- *(AC34.070: CAT II) The IAM will ensure certificates are used for authentication IAW DoDI 8520.2, PKI and Public Key (PK) Enabling.*

- *(AC34.075: CAT I) The IAM will ensure use of DoD-approved PKI digital certificates to authenticate requests for access to government information not approved for public release. For unclassified sensitive assets, the PKI certificate will be considered necessary but insufficient to provide authorized access.*

- *(AC34.080: CAT II) The IAM will ensure implementation of certificate-based logon to the NIPRNet using DoD-approved PKI as required by DoD policy. DoD-approved PKI will be required for SIPRNet when implemented in the future.*

- *(AC34.085: CAT I) The IAM will ensure a DoD-approved PKI certificate is used for logon to DoD Enclaves, networks, servers, desktop, laptops, and other network capable client devices. If PKI logon cannot be used, then a DoD compliant ID/password combination may be used and a migration plan implemented IAW JTF-GNO exception reporting requirements.*

NOTE: The PKI certificate is necessary but insufficient for access. Access must also require an active account and authorization.

- *(AC34.090: CAT I) The IAM will ensure PKI is required for the exchange of FOUO information with vendors and contractors, the DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority.*

- *(AC34.095: CAT I)The IAM will ensure DoD contractors who are not eligible for a DoD-approved PKI get and use digital certificates issued by approved external PKIs when interacting with DoD PK-Enabled information systems or accessing DoD restricted information and logical assets.*

- *(AC34.100: CAT III) The IAM will ensure Sas are trained on administration and implementation of PKI and PKE. At a minimum, this training will include:*

  – *PKI awareness training*
  – *How to configure systems for certificate-based logon*
  – *How to configure systems for digital signature*
  – *How to configure systems for email encryption*
  – *How to configure systems for Web server certificates*

DoD-approved PKI will be used for email and web services in accordance with the following.

- *(AC34.105: CAT II) The IAM will require certificate-based client authentication to restricted access (not public) DoD web servers using certificates issued by DoD-approved PKI certificate authorities.*

- *(AC34.110: CAT II) The IAO will ensure Browsers, including those that support software tokens, support the use of DoD-approved PKI, High Assurance Remote Access (HARA) solution (as appropriate for the classification level), or NSA certified solution for storing the user's certificates.*

- *(AC34.115: CAT II) The IAO will ensure DoD e-mail systems support sending and receiving e-mail signed by DoD-approved certificates. E-mail containing DoD sensitive or restricted information, are signed using DoD-approved certificates.*

Access to applications such as databases, Commercial-off-the-Shelf (COTS), and Government-off-the-Shelf (GOTS) software applications will be PK-enabled to the greatest extent possible. If PKI authentication is not yet required, migration plans should be in place. Newly purchased/acquired COTS and GOTS applications, network devices, and clients should be capable of supporting PKI based authentication. The Joint Interoperability Test Command maintains a list of products that have been tested to be interoperable with the DoD PKI. Additional information may be obtained from the JITC PKI website, http://jitc.fhu.disa.mil/pki/pke_lab/pke_index.html.

- *(AC34.140: CAT II) The IAM will ensure new Commercial-off-the-Shelf (COTS) software to be used in information systems that require PK-Enabling have passed interoperability testing performed by a DoD-approved PKI Program Management Office (PMO)-approved testing facility prior to procurement.*

3.4.3 Passwords , PINs, and Implementations of Something You Know

Passwords and PINs are similar; however, a password refers to a longer, more complex code, often consisting of both alphanumeric and special characters. IAW CTO 06-02, DoD is currently phasing out the use of passwords as a means of authentication to the NIPRNet and information systems connected to the NIPRNet in favor of using the higher assurance of digital certificates. Access to the NIPRNet and information systems connected to the NIPRNet which contain sensitive information will employ certificates issued by DoD-approved PKIs for authentication. However, some systems may not be PKI-capable. Other systems may not have a NIPRNet connection and thus, they cannot access the PKI CA to ensure timely updates and revocation information. Alternate Login Tokens (ALT) and ID/password are to be used only where PKI certificates cannot be implemented or the target user population has a documented exception to this DoD policy. This exception must be approved by the services/agency PKI PMO, the DOD PKI PMO, and the DAA. Howe ver, password configuration must comply with DoD policies and best practices. A common misconception is that the ID/password combination represents two factors. Use of a Logon ID with a single authenticator (password) or PIN represents one-factor authentication. The user password is the most commonly used form of authentication and it represents *something that you know*.

The more difficult it is for unauthorized individuals to guess or decipher the information that an authorized person knows and uses to gain access, the greater the assurance that access is controlled. Consequently, authentication methods based on *something that you know* are required to be difficult to guess and are changed periodically (as required by DoD policy) to make it difficult for an adversary to implement a successful “brute force” attack to compromise the system’s security. There is a trade-off between making PINs, passwords, and combinations difficult for unauthorized individuals to “crack” and making it easy for authorized users to remember. However, even the strongest password is inherently not secure because the authentication process requires it to be given to the authentication system making it subject to compromise via phishing or social engineering attacks.

Where passwords are used for authentication, these passwords may not be written down and stored in the vicinity of the computer. Automated technologies such as password protected screen savers must be used or the computer shut down if the authorized user needs to step away. Passwords used to protect access to classified data may be written and stored in a GSA-approved container or safe and accessed prior to logging onto the computer. The password must be returned to the GSA-approved container or safe after use.

Shared passwords mean that multiple people know or share the same "secret" used to protect the assets. Nonrepudiation is not possible in systems whose assets are protected solely by shared passwords. Furthermore, when one of the members of the group of authorized users is no longer authorized (e.g., they retire or change jobs), the password must be changed and redistributed. Although regular password changes normally enhance security, frequent password changes may itself present a more significant vulnerability. DoD policy requires use of individual passwords whenever possible for logical systems. Systems using shared or group authenticators must be approved by the DAA.

To further enhance password security some organizations may use one-time password generators or hardware tokens. With this system, each user is given a password generator that looks much like a pocket calculator. To access the central system, the user enters a PIN on the password generator to gain access to it; the password generator creates a random password (or number sequence) using a procedure that is duplicated at the central system. Further discussion on these devices can be found in a later section.

- *(AC34.168: CAT III) The DAA will ensure ID and password access for system and network access is used only where use of DoD PKI is not technologically feasible, cost prohibitive, or is deemed unwarranted. Exceptions to the PKI policy must be documented; DAA approved; and coordinated with the service/agency PKI PMO as well as the DOD PKI PMO.*

- *(AC34.170: CAT II) The IAM will ensure where passwords are used for access to DoD restricted assets (i.e., networks, workstations, or applications), at a minimum, passwords are created and changed in accordance with current DoD policy. Users must be trained on this requirement and, if possible, an automated procedure must be in place to enforce these rules.*

- *(AC34.175: CAT I) The IAO will ensure default installation passwords are removed from installed devices used for production such as communications, databases, applications, or operating systems.*

- *(AC34.180: CAT II) The IAO will ensure individual users and system, application, and database administrators use individually assigned accounts rather than a group or shared accounts or authenticators.*

- *(AC34.181: CAT II) The IAO will ensure group or shared authenticators for application or network access are used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD-approved PKI has been explicitly approved by the DAA.*

- *(AC34.185: CAT II) The IAO will ensure shared/group PINs and passwords are used only in accordance with the DoDI 8500.2. Auditing procedures are implemented in conjunction with these methods to support nonrepudiation and accountability.*

3.4.4 Hardware Tokens

Hardware tokens (also called hard tokens or eTokens) are hardware devices with computing capability integrated into the device. As with biometrics systems, these devices can be integrated into either a physical or logical access control solution depending on the technology implemented on the token. For example, validation of the possession of a valid token can be used for access when low assurance is adequate for physical access but storing a user's private key on a token such as the CAC increases the overall assurance because the adversary now needs an additional item (the token) to breach the system.

These devices include smart cards and Universal Serial Bus (USB) cryptographic tokens. Use of hardware tokens, which contain tamper protections such as zeroization of contents and tamper detection switches, is essential. When hardware tokens require the user enter a PIN, their use represents two-factor authentication, *something you have* and *something you know*. Tokens such as USB key chain tokens which generate a passcode simply by pushing a button on the device represent single-factor authentication, *something you have*. Tokens come in various shapes, sizes, technologies, and can perform various functions. Not all cryptographic modules are in separate hardware tokens. Some are implemented in software (commonly called software modules). Many applications and operating systems have software modules (e.g. Microsoft XP, Netscape). Software modules do not provide as high a degree of security as hardware.

NOTE: See also the Alternative Logon Token section for requirements for non-CAC hardware tokens used to hold DoD PKI for access to DoD sensitive information. These tokens must be approved using the Alternative Logon Token approval process.

- *(AC34.189: CAT II) For information systems with DoD sensitive information that are not currently capable of connection to NIPRNet (cannot use PKI authentication), the IAM will ensure, at a minimum, users are authenticated to their CAC, DBIDS, or other DoD issued identification card prior to issuance of a non-CAC hardware token for use to login to DoD sensitive information assets.*

- *(AC34.190: CAT II) The DAA must document and certify that the system is incapable of connecting to the NIPRNet; ensure the system is compliant with all applicable STIGs; document coordination with the service/agency PKI PMO; and document plan for migration and mitigation of residual risk.*

- *(AC34.160: CAT I) The IAM will ensure if the hardware token is used as an identity credential to support access to classified assets, it is combined with, at a minimum, a PIN and/or a biometric verification.*

- *(AC34.205: CAT II) The IAO will ensure the information system (network device, desktop, laptop, handheld, etc.) is configured to lock the device when the session is left unattended. This requirement matches the existing workstation requirement for the password-protected screen saver for unattended devices. Alternate solutions for ensuring an authenticated session is not left unattended by the user once the token is removed must be approved by the DAA.*

- *(AC34.210: CAT II) The IAO will ensure users are trained on the proper handling and security procedures for DoD-issued hardware tokens, used to enable access to sensitive information.*

3.4.4.1 The DoD Common Access Card

The CAC is an integrated identity and access control solution. It is not possible to discuss integration of physical and logical access control without a thorough understanding of the scope of access control techniques that can be leveraged using this one device. The CAC will be the principal card used to enable physical access to controlled areas and assets on the Department's computer networks. Sites are not required to discontinue use of non-CAC access control solutions; however, a migration plan showing a timeline for future compliance with DoDI 8520.2 must be documented. Additional (local) credentials may be used to support access control if deemed necessary by the local Security Manager. However, in accordance with the policy, the CAC will remain the principal identification credential. Issuance of local credentials must include identity-proofing using the CAC and the Defense Eligibility Enrollment Reporting System (DEERS) database. Policies for issuance of local credentials are discussed in subsequent sections.

The CAC holds certificates and associated private keys issued by the DoD PKI to DoD eligible users. Note that certificates issued by the DoD PKI are not only issued on CACs, and certificates issued by external DoD-approved PKIs do not use the CAC as discussed in a previous section.

It is important to note that the DoD CAC is a composition of commonly used access control technologies. These technologies integrate easily into GOTS and COTS products that use standard industry protocols. Integration of the DoD CAC, PKI and other technologies on the CAC should be an integral part of the access control solution to meet current and future security requirements and are mandated by government policies.

Figure 3-1 depicts the layout of the CAC and highlights the purpose of its components. Note that it is not meant as an exact depiction of the currently issued CAC but serves only to illustrate the technologies discussed herein. The CAC currently has many demographic data elements stored in its integrated circuit chip (ICC). Most of these elements are also printed on the card. A cryptographic co-processor and secure storage supports the DoD-approved PKI functionality. The complexity of the microprocessor is the primary distinguishing feature between a smart card and a memory card. The CAC's barcodes and magnetic stripe store data that can be used by various DoD applications, thus, the CAC can also be used as a memory card. The magnetic stripe has no data encoded on it at issuance. Organizations may use standard magnetic stripe technology to write data to the magnetic stripe. Most applications using the ICC will use the

CAC to establish user authentication and trusted communication channels, but application data will reside in remote databases.

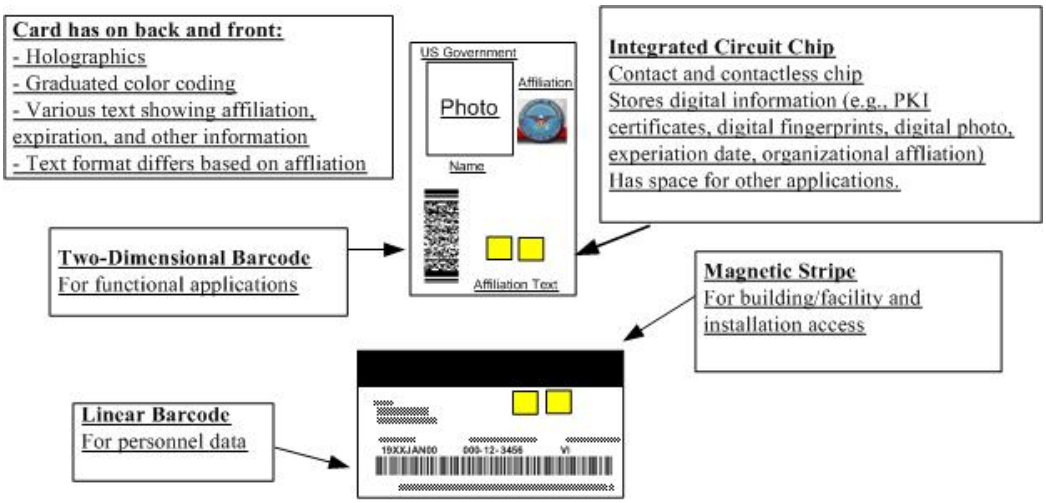

Figure 3-3. Generic Depiction of CAC Layout

NOTE: Title 18, US Code, Section 701 prohibits photographing or otherwise reproducing of departmental ID cards in an unauthorized manner. Thus, the above document is not intended to be an exact depiction of the DoD CAC which will be changed with the approval of new DoD policies and standards.

To access the data or certificates on the chip, a PIN must be entered. The card has a routine that locks the card after three incorrect PIN attempts. To reset and re-enable the card, the cardholder must return to a CAC issuance or reset workstation, present the card and proof to support validation of the cardholder's identity. In addition to the issuance terminal (RAPIDS) card can be reset at a CAC PIN Reset (CPR) terminal. Validation of the card owner's identity should include verification of his or her fingerprint against biometric reference data stored in the DEERS.

If an adversary found or stole a CAC and guessed the required PIN, he or she would have access to the digital certificates, cryptographic functionality, and other information either on the CAC ICC or accessible by use of the CAC. Certificates on CACs that are lost or stolen or on CACs held by personnel in specific personnel categories (e.g. Prisoners of War or Missing in Action) shall be revoked in accordance with DoD's certificate revocation procedure

The CAC can be used as purely an identity card, where the force protection officer or other attendant is trained to verify that the cardholder is in possession of his or her own CAC, that the CAC is valid, and to allow or deny access in accordance with local access control policy. In an automated system, a card reader is installed at the access control point to read the stored identity information from the card's memory. The name or unique identifier is then checked in DEERS or other access control database. In each case the card is checked for expiration or revocation. This method represents single-factor authentication (*something that you have*, i.e., a CAC). Use of a memory card (*something that you have*) can only support public access of physical or logical

assets, since a memory card does not meet the DoD minimum standards requiring multi-factor authentication for access to DoD protected assets.

To achieve a higher level of assurance, a keypad or keyboard can be installed at the access control point. The user presents the card to the card reader and then enters a PIN. This usage represents use of two-factor authentication or *something that you have (CAC)* and *something that you know (PIN).*

Biometric data in the form of the photograph and fingerprints are collected during the enrollment process and are stored not only in DEERS (biometrics will also be stored on the PIV version of the CAC in the future). The fingerprint data is stored in encrypted form and is unlocked with the user's PIN. Using the biometric reference data stored on the ICC requires installation of a biometric reader at the access control point. Use of the fingerprint biometric comparison in combination with the CAC and the PIN, would represent use of three-factor authentication or *something that you have (CAC), something that you know (PIN),* and *something that you are (*biometric comparison). However, it may not be practical at a busy gate to have users enter a PIN to access PKI or Biometric Data. It may be more effective to place this technique closer to the asset.

3.4.4.2 Alternate Login Token

DoDI 8520.2 states that all DoD networks required by DoDD 8500.1 to authenticate users will perform this authentication using certificates issued by DoD-approved PKI on hardware tokens. The CAC is the preferred hardware token but there are special instances where the certificates issued on the CAC cannot be used to perform various missions. For example, the DoD requires that system administrators have separate logon credentials based on role and least privilege. These individuals perform both administrator functions and normal user functions and need different privileges assigned depending on their role at the time of authentication. Hardware. To accommodate users with multiple roles, the DOD CIO has approved the use of the Alternate Login Token (ALT). The Alternate Logon Token Memorandum, dated August 14, 2006 authorizes the use of hardware tokens other than the CAC to be issued with DoD-aproved PKI certificates.
The ALT must be issued using the alternate logon certificate process. Each service/agency has defined a process for how they will be issuing alternate tokens to their users. This process must be documented in the service/agency level Certificate Practice Statement (CPS). The initial population to be issued the alternate token is the system administrator community. Sites wanting a particular category (such as flag officers, on site volunteers, foreign nationals, etc.) added to receive the ALT, must request this through their service/agency PKI PMO who can submit an updated CPS to the DoD PKI PMO. This update must include the modified Registration Authority (RA) Certification Practice Statements (CPS) Addendum. This addendum must be reviewed by the DoD PKI Certificate Policy Management Working Group (CPMWG) before approval.

The intention of the ALT process is not to provide a static list of pre-approved devices which accommodates all missions, but to allow the C/S/A to tailor solutions to the mission. The ALT approval process ensures standardized implementation of the alternative X.509 certificate

(including certificate names, operational requirements and processes). This process also guards against the proliferation of non-standard or low-assurance hardware tokens.

- *(AC34.215: CAT II) For authentication to NIPRNet and NIPRNet connected systems where DoD-approved PKI issued on an alternative (non-CAC) hardware token is required, the IAM will ensure use of a DoD-approved hardware token. Use of alternative hardware tokens are limited to particular categories of uses approved by the DoD PKI PMO and documented in the service/agency Certificate Practice Statement (CPS) and addendum.*

3.5 Physical Access Control Methods

Although this document is focused on access control for IT systems, a true integrated access control solution should consider physical security controls when assessing the security protections needed to secure the logical asset. Logical security assessment should not occur in a vacuum but should be a combined effort between the physical and logical security teams. This section, therefore, is provided as background for the information assurance manager in an effort to educate and encourage the leveraging of physical security techniques in layered asset protection.

Physical access control methods are must be used in conjunction with the logical access control methods discussed above to satisfy assurance requirements for personal authentication. Physical security measures can be active or passive and may include attendant personnel, physical barriers, electronic countermeasures, monitoring, and automated entry systems. While biometric and token readers can be integrated into information technology access control points to support two-factor or three-factor authentication, this is not always cost-effective, practical or the solution desired by the asset owner. Furthermore, DoD has a unique advantage in physical access control methods (force protection personnel) that can and should be leveraged to protect DoD assets. While the focus of this STIG is information systems, some of the assets to be protected are tangible, physical assets. Information systems include hardware such as hard drives, backup tapes, laptops, cabling, computer room facilities, and mobile or remote devices. Protection for these devices must include physical controls. Information Assurance solutions should include a consultation with the physical security specialists and an assessment of the environment by these specialists. The information in the following subsections is thus provided as an orientation of physical security considerations for the information assurance manager. Whether these techniques and technologies are employed as part of the solution will depend on the specific asset, risks, and environment but the IAM should ensure that they consider physical security as part of security in depth.

3.5.1 Classified Storage and Handling

Protection of sensitive and classified assets must include classified storage, proper security marking, transportation, destruction, and incident handling. These requirements for access control are fully established by DoD policies and must be strictly followed because of the high value of the assets. DoD 5200.1-R provides physical protection standards for the storage of classified information. The requirements in this regulation provide the only acceptable combinations of access control methods for the protection of classified material and equipment.

Director Central Intelligence Directive (DCID) 6/3 and 6/9 provide guidance for the protection of Sensitive Compartmented Information (SCI) material and equipment.

GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. Storage of classified material and equipment such as hard copy documents or removable hard drives must use GSA approved containers only. Containers must be equipped with a three position, changeable combination lock meeting the Federal Specification (FEDSPEC) FF-L-2740.

Physical access points to facilities housing networks and workstations that process or display classified information (Top Secret or Secret) must be guarded and/or alarmed 24 X 7 in accordance with 5200.1R. Intrusion alarms must be implemented and monitored with response times appropriate to the classification of the materials protected. To gain access at the access control perimeter of facilities or workplaces processing classified information, two-factor authentication is required. This requirement can be met using visual monitoring by an attendant or through use of an automated entry system (discussed in a subsequent section). Either automated or manual classified access logs should also be maintained to ensure accountability. (Note that not all classified assets are protected by a facility layer.)

All levels of classified (Top Secret, Secret, Confidential) materials must be properly marked. Transportation of classified assets must use approved and authorized couriers and/or requires use of proper cover sheets and envelopes as required by DoD policy.

- *(AC35.025: CAT III) The Security Manager will ensure all physical security controls, including security marking, handling, and facility procedures required for the protection of information systems and associated hardware devices comply with the requirements of the DISA Traditional Security Checklist.*

3.5.2 Attended Access

The entry control perimeter should be under visual control at all times during working hours to prevent entry by unauthorized personnel. This requirement may be accomplished using an attended access control method (e.g., guard or monitored video surveillance system). During non-working hours, random guard patrols throughout the facility or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets are used depending on the classification of the information being protected.

Attended access control can increase the security stance at any security perimeter layer. In many cases, manual access control methods are the critical components to access control in support of DoD missions. Attendants can be force protection officers, private security guards, or other authorized individuals assigned to monitor access control points and controlled areas. These attendants may also be authorized as trusted agents to facilitate access by emergency personnel requiring access to the controlled area after hours and/or during emergency situations. Attendants must be trained to verify identity credentials to the level of assurance required.

Attendants must have the tools necessary to complete the access control task such as authorized personnel roster; phone lists, emergency contact information, and should be able to trigger facility alarms, when necessary. For increased assurance in the workspace, authorized attendants can patrol the area or monitor remote video of vulnerable points in the perimeter.

Attended access control can be implemented as a single-factor as a part of a multi-factor authentication solution. Examples of single-factor authentication using attended access includes: having the attendant verify the authenticity of a set of hand-carried orders or a CAC; verifying that the person requesting access knows a shared combination; or having the attendant allow only individuals that he/she personally recognizes. More importantly, attended access control enables two-factor authentication by training the attendant to take the following actions.

- Comparing a cardholder to the image printed on a badge/card (*something that you are* and *something that you have*).

- Comparing a cardholder to an image pulled from a database by use of a card, PIN, or biometric system (either *something that you are* and *something that you have* or *something that you are* and *something that you know*).

- Checking the security or anti-counterfeit features on a card presented for use (increased assurance of *something that you have*).

Using guards to oversee proper use of the personal authentication and protective barrier systems can mitigate many access control system vulnerabilities. An attendant could deter an adversary from using a lost or stolen memory card for unauthorized access. Furthermore, an adversary trying to use an artifact to spoof a biometric system could be deterred by an attendant.

- *(AC35.010: CAT II) The Security Manager will ensure attended access control (e.g., guards and video surveillance systems are implemented in compliance with the policies of DoD 5200.1-R.*

3.5.3 CAC and DBIDS for Physical Access Control

Although the Federal PIV and DoD CAC (discussed in a previous section) is the primary card used for physical access, individuals may be authorized access to DoD assets but are not elible to receive a CAC. The Defense Biometric Identification System (DBIDS) card can be issued to these individuals but can allow access only to a single DoD installation or facility. The DBIDS card, while not an interagency PIV credential, has a similar identity-proofing process is required for permanent issuance of the DBIDS credential. The current plan is to eliminate all other non-FIPS 201 compliant badges and associated equipment used for physical access once the PIV, CAC, and DBIDS are fully deployed. However, existing legacy Physical Access Systems (PAS) will continue to operate until upgraded or replaced.

3.5.4 Supplemental Badges, Memory Cards, and Smart Cards

In accordance with DoD policy, the CAC is the required identification credential that will be used DoD-wide to support physical access control. Based on the multiple technologies on the

CAC, the CAC can also be used as a DoD badge, memory card, or smart card. However, it is important to note that DoD policy also allows for the issuance and use of supplemental badges to accommodate special access requirements. Supplemental badges, tokens, and smart cards may be used where existing automated access control applications are not readily convertible for use with CAC technology; when individuals requiring access are not eligible for the CAC; or when the local Security Manager determines that it is required based on special mission requirements (e.g., identification and physical access for restricted areas). "A National Agency Check with Inquiries (NACI) or equivalent national security clearance (NACLAC) is required for permanent issuance of the Federal PIV credential such as the DoD CAC. Occasional visitors to Federal facilities will continue using a locally established, temporary issue, identification system. Credentials issued to individuals without a completed National Agency Check with NACI will be electronically distinguishable from those credentials revealing a completed NACI" (IAW Draft DoD 5200.8-R). Locally issued badges and cards must be combined with other authentication methods for access to classified or sensitive areas or information.

- *(AC35.053: CAT II) When using locally issued badges, the Security Manager will comply with applicable DoD policies governing identity cards and with policies in the Identification Credentials section of this STIG.*

- *(AC35.055: CAT I) The IAM or Security Manager will ensure DoD personnel and contractors are positively authenticated before granting access to DoD protected assets or prior to issuance of any locally issued or supplementary authentication credential used to support access control.*

- *(AC35.056: CAT II) The Security Manager will ensure supplementary badges, memory cards, and smart cards issued to individuals without a completed National Agency Check with NACI are electronically distinguishable from those credentials revealing a completed NACI (IAW Draft DoD 5200.8-R).*

- *(AC35.060: CAT II) The Security Manager will use badges, memory cards, and smart cards (something you have) to protect unclassified, non-sensitive assets. This requirement includes use of the CAC when used only as a badge without requiring authentication by PIN or biometric.*

- *(AC35.065: CAT II) The Security Manager will ensure audit logs of badge, memory card, and smart card issuance, revocation, and collection.*

3.5.4.1 Badges

Badges come in various forms and support varying levels of personalization. Personalization methods include badge-holder identifiers, including the photograph, security clearance, and signature. As badge personalization elements increase, more effort is needed to identity-proof the badge before issuing. Locally produced badges must comply with DoD policy as discussed in previous sections. DoD badge types include color-coded (non-personalized) badges, enumerated badges, and personalized badges.

A color-coded badge is often used to identify visitors requiring an escort within a building or workspace. Risks are increased if authorized personnel do not strictly adhere to any required escort policy. When the CAC is used as a badge, color is used to differentiate between Government and contractor staff.

Enumerated badges are usually issued after presentation of proof of identity and verification against a list of authorized visitors. Sometimes the visitor is asked to exchange their identification credential, such as a drivers' license, for the numbered badge at the access control point. The badge is exchanged for the identification credential upon exit.

Personalized badges require an identity-proofing process. These cards include verified identifying information such as the badge holder's name, photograph, and signature, which can be used to authenticate the cardholder.

Color-coded, enumerated, and personalized badges provide the Security Manager with minimal personal authentication assurance because badges are easily copied, stolen, or counterfeited using readily available technology. While the adversary needs greater skill to alter or counterfeit a personalized badge, these skills are common and the costs are low. Where increased security assurance is required, the badge should be combined with additional authentication methods as those discussed in subsequent sections.

3.5.4.2 Memory Cards

Memory cards are data storage devices. These cards allow storage of information used for personal authentication, access authorization, card integrity, and applications. The card does not process information but serves as a repository of information. The data can be written to a magnetic stripe, bar code, or optically stored on the ICC. When a smart card is used as a repository of information without requiring the cardholder to input a PIN or present a biometric reference sample, the smart card is implemented as a memory card. This method is often used for "touch and go" access and does not provide a high level of assurance since the wireless transmission can be easily intercepted. Locally produced memory cards must comply with DoD policy as discussed in previous sections.

If a user presents a memory card to a reader and enters a valid PIN using a keypad or keyboard, two-factor authentication is employed. If the access control application determines that the PIN is valid and corresponds to the memory card presented, then the user is allowed access privileges based on *something that he or she has* and *something that he or she knows*.

3.5.4.3 Smart Cards

A smart card has one or more ICCs. It can also store data using memory chips on the card. The difference between a smart card and a memory card is that the smart card processes data like a simple computer. Communication with a smart card can be via contact or contactless (proximity) interfaces. At an access control point, the smart card is presented to the reader. Many applications require the cardholder to enter a valid PIN to enable smart card and cardholder authentication and subsequent establishment of a secure communication channel between the smart card and an external application for authenticated users. This type of access

represents two-factor authentication comprised of *something you have* (a smart card) and *something you know* (a PIN).

DoD is implementing smart card technology through use of the CAC, however local applications may require use of a supplemental smart card. Locally produced smart cards must comply with DoD smart card policy as discussed in previous sections.

3.5.5 PINs, Combinations, and Other Forms of Something You Know

A PIN is a numeric code entered using a keypad. The user PIN is a commonly used form of authentication that represents *something that you know*. *Something that you know* may include:

- A PIN or password,
- Mother's maiden name,
- The name of your first pet,
- A safe combination, or
- A procedure such as "push the # key, enter your password, push the * key, wait until the blue light comes on and push the # key".

The more difficult it is for unauthorized individuals to know, guess, or decipher the information that an authorized person knows and uses to gain access, the greater the assurance that access is controlled. Consequently, authentication methods based on *something that you know* are required to be difficult to guess and are routinely changed to make it difficult for an adversary to use a "brute force" attack to compromise the system's security. There is a trade-off between making PINs, secrets, procedures, and combinations difficult for unauthorized individuals to "crack" and making it easy for a user to remember it. If the authorized user has to write down the "secret" then the protected asset is vulnerable.

PINs or combinations used to protect access to classified data may be written and stored in a GSA-approved container or safe and accessed prior to logging onto the computer. The documented secret should be returned to the GSA-approved container or safe after use.

Assets stored in areas with public or heavy traffic by unauthorized individuals such as building entry lobbies, are at increased risk. Consequently, "secrets" that protect these assets must be diligently protected by secure PIN and/or combination controls and procedures.

Shared PINs and safe combinations mean that multiple people know or share the same "secret" used to protect the assets or to protect access to an area wherein the protected assets are stored in the open. Nonrepudiation is not possible in systems whose assets are protected solely by shared PINs or combinations. Furthermore, when one of the members of the group of authorized users is no longer authorized (e.g., they retire or change jobs), the shared PIN or combination must be changed and redistributed. Although regular PIN and combination changes normally enhance security, too frequently changing passwords may present disrupt mission effectiveness or even introduce system vulnerabilities.

- *(AC35.010: CAT II) The Security Manager will ensure, at a minimum, PINs and combinations are created and changed in accordance with the DoDI 8500.2. Users are trained on this requirement and, if possible, an automated procedure is in place to enforce these rules. (This is not applicable for PKI PIN).*

- *(AC35.015: CAT I) The IAO will ensure default installation PINs or combinations are changed when installing devices used for production such as GSA-approved safes or combination locks.*

- *(AC35.020: CAT II) The Security Manager and IAO will ensure shared/group PINs and combinations are used only in accordance with the DoDI 8500.2. Auditing procedures are implemented in conjunction with these methods to support accountability.*

3.5.6 Physical Tokens

Physical tokens consist of keys and unique documents such as DoD hand-carried orders. Access control methods used for single-factor personal authentication in DoD include simple physical keys, 3-plane (complex) keys, and hand-carried orders. These tokens are authorized for the protection of non-mission critical, unclassified, non-sensitive assets. Like PKI, physical tokens represent *something you have*. Unlike PKI, they provide a low level of assurance and are only suitable for use when protecting assets with low risk and low confidentiality level.

Simple physical keys provide minimal protection and assurance, as they are highly susceptible to copying or theft. Furthermore, the locks controlled by simple physical keys, are relatively easy to compromise. Most key systems authorized for use in government facilities, use a higher security lock and key, which is harder to manipulate and use keys that are difficult to copy. A 3-plane (complex) key is one of the more secure key systems since the keys themselves are more complicated to copy, blank key stocks are not readily available to adversaries and are more difficult to counterfeit, and the locks controlled by 3-plane keys are more difficult to compromise. Organizations must purchase keying systems from authorized GSA sources only. Key control policies and procedures, that address where the blanks are strictly controlled, can also mitigate this risk. Any key used is highly susceptible to theft and use by an unauthorized adversary.

- *(AC35.025: CAT III) The Security Manager will ensure all physical security controls for the protection of information systems and associated hardware devices comply with the DISA Traditional Security Checklist.*

NOTE: This includes the following:

- If physical keys (regardless of type) are the only access control method (single factor authentication) used, they only allow access to unclassified, non-sensitive non-mission critical systems (e.g., public web sites).

- Hand-carried documents will not be used as a single-factor authentication method for access to sensitive or mission critical systems.

– Authorized personnel validate the identity of the person presenting hand-carried documents and the documents themselves prior to granting access to to DoD controlled systems.

3.5.7 Physical Intrusion Detection Systems

Physical intrusion detection systems are electro-mechanical devices used at all layers of the security architecture to monitor, detect, and notify responsible personnel of physical or logical attacks. These devices include features such as remote video monitoring, alarms, motion sensors, and logging/reporting capabilities. Once notified Physical Security personnel must follow established response procedures as dictated by DoD policy and the specific attack underway. In addition to intrusion detection systems, exit and entrance control procedures and user training are essential to detecting unauthorized personnel in the controlled space.

Remote video enables centralized monitoring of the perimeter or controlled space. Authorized personnel can monitor the displays and alarming systems and react accordingly. Remote video can also be used where authorized individuals or pre-registered visitors present identity credentials to the reader and the attendant can remotely compare the video image and text transmitted by the smart or memory card to an authorized access control list before granting/denying access.

Physical intrusion detection systems can be used to detect and deter unauthorized physical access and alert guards to attempted breaches of the perimeter. Sensors can be installed at many points around and within a controlled perimeter. Environmental factors should be considered when developing the optimal strategy for any given solution. For example, motion detection sensors in areas with abundant wildlife may cause frequent false alarms and are, consequently, ineffective. Systems should be physically protected within the workspace and accessible by a few authorized personnel to ensure the integrity of these automated methods. Electrical systems supporting these devices must also be protected by an emergency back-up power plan.

Unauthorized access attempts at automated gates should alarm guards and prompt the indicated response based on threat assessment. In addition, alarms should be installed such that tampering with keypads and readers of access control systems will trigger an alarm. Requirements for physical intrusion detection system are found in DODD 5200.

3.5.8 Other Physical Security Considerations

The following discussion is included to give backbround on the need information assurance specialists to consider issues related to unauthorized physical access and the risk of electronic emanations as part of the security solution. A risk assessment for protecting a logical asset such as data should include working with the Security Manager or physical security representation to determine what controls can/should be layered as part of an integrated security solution.

If the access control perimeter is located at the Building Layer, the Security Manager must ensure doors, windows, loading docks, garage entrances and exits, sewer and roof accesses, balconies, and fire escapes are secured appropriately. Trees, trellises or textured walls provide an

adversary access to a second or third story window or balcony, and must be considered in assessing risk. Authorized individuals and users in the workspace must report broken windows and security doors and people without required credentials encountered within controlled perimeters. Local policies and procedures must be in place to address tailgating whether the practice is allowed or not.

The surfaces of rooms, including walls, windows, ceilings, vents, and roofs are not constructed primarily as security barriers, however, they must be factored into the Security Manager and IAM access control strategy. Sound abatement between protected areas where sensitive or classified discussions take place must be considered. Sound travels effectively through ventilation shafts and can transmit through ceilings, floors, and walls. A security professional should be employed to assist in analyzing sound abatement requirements. Unauthorized physical access through drop-down ceiling panels, attic access doors, raised floors, windows, or ventilation shafts should be obstructed. The threat of unauthorized visual access including the use of reticulating fibers or remote cameras must be considered when designing workspace protection for classified or mission critical assets. Requirements for security windows, walls, and door should be coordinated with the Physical Security Manager.

This page is intentionally blank.

4. BIOMETRIC SYSTEMS

Historically, biometrics has been relegated to a single method (fingerprinting). However, new biometric methods and technologies have been developed that lower cost and increase usability. Companies developing new methods number in the hundreds and their methods continue to evolve as the technology advances. The availability, effectiveness, and affordability of biometric technology continue to progress as the demand for authentication has increased. This increased interest is driven by an exploding problem with identity theft and computer fraud coupled with the increased use of remote connectivity methods, such as, Internet access.

Biometric data is now captured on passports and as part of the military service record. Central biometric repositories are planned for the DoD space, which will facilitate the rapid adaptation of biometric technology for both battlefield applications and support services. These systems are often used within buildings to protect access to workspaces where environmental effects on performance can be optimized for sensitive electronics. Although biometric authentication systems can be used to enhance security, there are security risks associated with the use of any technology, which must be mitigated. A compromised password can simply be changed, however once a biometric is compromised there is no going back or changing it. For information systems that currently accept Biometrics-only for authentication, this must be combined with another authentication method such as a password in accordance with DoD-approved PKI policy. Also, a migration plan for DoD-approved PKI authentication must be documented.

4.1 Biometric Technology and Terminology

With regard to technology, biometrics is the term given to the use of biological traits or behavioral characteristics to identify an individual. The trait used may be fingerprints, hand geometry, facial geometry, retina patterns, iris patterns, voice recognition, handwriting recognition, or any of the increasingly available traits. A biometric system is essentially a pattern recognition system. The system includes all the hardware, software, and the interconnecting infrastructure, which enables the matching of a live sample to a stored pattern in a database.

Biometrics technologies compare biometric samples to form an opinion of whether or not a person is known to the system. This opinion is most often rendered in a “match” or “nonmatch” decision, based on a predetermined threshold of confidence. In addition to this decision, some biometric systems return a score in addition to the decision, while others (particularly, facial recognition systems) return a rank ordered set (highest confidence to lesser confidence) of potential matches to the interrogator.

Positive biometric verification can be either a component of physical or logical access controls. Physical access refers to entry to a secure area such as a building or server room. Logical access refers to use of a computing resource such as desktop computer. The biometric hardware and software to support physical and logical access control can be and often are identical. In both cases, the biometric system captures a biometric sample from the user, compares it against a biometric reference data, and either verifies that the two are the sufficiently similar to be considered “a match” or that they are not (“non-match”). Some biometric systems are easier and more convenient to use than others, depending upon the application environment. Some biometric systems require user cooperation; others can be implemented covertly (for example,

"face in the crowd" applications). Not all biometric types and applications are acceptable for use in DoD; therefore, the Security Manager should consult with resources, such as with the Biometrics Management Office (BMO), as part of the design and selection process for biometric applications.

Biometric systems are fundamentally different than other types of personal authentication systems for the following reasons. Depending on the implementation, it may be far easier for an adversary to know a complex, machine-generated PIN that has been written down for use by an authorized user or to steal or counterfeit a smart card, than it is for an adversary to successfully overcome a biometric system. The level of difficulty increases further the solution includes an attended access control. Because of the unique skills required, fewer adversaries exist for biometric systems. However, controls are still needed to ensure the integrity of the biometric reference database and implementing attended enrollment. Because it is easier to change a compromised password or smart card than a user's biometric, it is critical that the enrollment process is tightly controlled to ensure unauthorized users do not become part of the verification database.

Depending upon the biometric technology and the risk environment, using biometrics as a replacement technology may either improve or degrade security. Using biometrics to supplement the other authentication factors will very likely enhance security. Accordingly, from a security perspective, biometric verification is best deployed as a component of two-or three-factor authentication.

4.1.1 Identification versus Verification

Biometrics can support either *identification* or *verification*. When biometrics is used in the identification process, users do not state who they are. For example, a fingerprint reader might be used to identify criminals who otherwise might refuse to identify themselves or present false identities. In the future, iris-scanning devices might be able to identify known terrorists in a crowd. When biometric technology is used in identification, the process is *one-to-many*. In other words, one reading must be compared against many potential profiles to find a possible match.

When biometrics is used in the verification process, users first declare who they are by entering their logon name (in the case of most computer logons) or presenting an identification card (most common in physical access control). Then biometric technology is used to *verify* that identity. The technology does this by comparing a biometric reading against a profile stored *for that user*. In this case, the process is considered to be *one-to-one*. That is, one reading is compared to one profile – they either match or they do not.

Identification processes are significantly more complex and error prone than verification processes. Biometrics technologies are *indicators* of authentication assurance with results based on a predetermined threshold with measurable (not theoretic) False Accept Rates and False Reject Rates. A biometric result should not be interpreted as proof of identity. From a security perspective, biometric verification is best deployed as a component of two-factor or three-factor authentication.

4.1.2 Enrollment

Initial Verification of Identity happens when the user presents some evidence that he or she is in fact that individual without using the biometric technology for this verification. This might involve the presentation of photo ID or authentication to trusted computer. All subsequent verification of identity is dependent upon the strength of this initial verification. In other words, if an imposter can present a false identity at this stage in the process, he will be able to authenticate the impersonated identity in perpetuity unless there is some alternative means of detecting the false identity. The stages are: Capture, Extraction, Package Creation and Assurance, and Package Storage.

- In the Capture stage, biometric technology is used to record a user's physical characteristic or behavior. The hardware performing the reading is called the *capture device*. Capture devices typically are designed to capture one biometric characteristic such as a finger print, retina pattern or keyboard dynamic.

- In the Extraction *stage*, the captured information from the capture device is translated into a digital representation of the biometric characteristic. This digital representation is known as the *biometric template*.

- In the Package Creation and Assurance stage, the biometric template is associated or bound with the user's identity information (e.g., name, ID, etc.). The package is then encrypted and digitally signed to protect its integrity and confidentiality.

- In the Package Storage stage, the biometric package is encrypted and signed package the written to a non-volatile storage medium for future use in the verification process. This storage medium may or may not be integrated into the biometric system. For example, packages might be transferred to a smart card or external database.

4.1.3 Verification

The stages of the verification process are as follows.

Identification – the user presents some form of identity, perhaps typing in a user name or ID number. Alternatively, the user could present a swipe card or smart card.

Capture – this is the identical process as the one performed during enrollment.

Extraction – this is also the identical process as the one performed during enrollment, but this time the result is called the *live sample* rather than the biometric template.

Package Retrieval and Validation – the biometric package is retrieved from storage and decrypted. Its digital signature is validated to ensure that it was created during the enrollment process and not modified since then.

Comparison – The live sample and biometric template are provided as inputs to a software module known as the comparator, which generates a score describing how close a match the two

are to one another. Based on predetermined thresholds, the two are either declared a match given the resulting score (*acceptance*) or they are not (*rejection*). The determination is forwarded to whatever access control system the biometric technology is supporting.

4.2 Separation of Duties

With biometric access control technology, administrators are the only users that interact with the system beyond the biometric capture device. This distinguishes it from most other technologies (operating systems, web servers, databases, desktop applications, etc.) in which users enter, manipulate and retrieve data on a regular basis. Any user action represents a potential point of vulnerability. Thus, in the case of biometrics, improper administrative user access poses one of the greatest security risks to the system. Biometric system administrators are required to authenticate to the biometric software before the software allows any access to its controls. This authentication should be something other than biometric authentication (e.g., a password, perhaps combined with a token or smart card) in case the biometric system has been compromised or is not functioning.

Ideally, there should be a separation of duties within the administrative function. As specified in the *Biometric Verification Mode Protection Profile for Medium Assurance Environments*, there should be, at a minimum, the following three administrative roles:

Enrollment Administrator – the individual who verifies the identity of new users and guides them through the creation of their associated biometric reference templates using the biometric capture device.

Security Administrator – the individual who establishes and modifies the values of configuration parameters in the biometric software.

Audit Administrator – the individual who reviews audit logs for security violations and related suspicious behavior.

The integrity of the system may be impacted if these roles are combined. For example, if there is no independent audit administrator, then other administrators can tamper with the system without detection. If the security administrator is also the enrollment administrator, then he or she can manipulate configuration settings to allow for weak templates and then enroll users in a manner that will make it easier to breach the system at a later date. If there is separation of duties, then this is not possible unless the enrollment and security administrators conspire to jointly circumvent the system controls.

If the biometric software supports separation of duties as described above, the security administrator should activate this feature. If not, the IAO should still implement compensating controls to mitigate this risk using administrative procedures. For example, the IAO can regularly check that each user enrolled in the system has an approved System Authorization Access Request (SAAR) DD Form 2875 or similar access authorization forms used to request that access. In addition, audit logs can be regularly copied to a location inaccessible to biometric systems administrators so they can be reviewed independently.

- *(BIO1010: CAT II) The IAO will ensure individuals are assigned in writing to the following administrative roles: Enrollment Administrator (enroll or re-enroll users); Security Administrator (modify the security configuration), and Audit Administrator (review and manage audit logs).*

Preferably, the biometric software will have its own administrative authentication module. If this feature is not available, the systems administrator should limit permissions (to the greatest extent possible) to all executable files to a user group whose membership consists of authorized administrators only.

- *(BIO1020: CAT II) The IAO will ensure the following functions are restricted to authorized Administrators:*

  - *Creation or modification of authentication and authorization rules*
  - *Creation, installation, modification or revocation of cryptographic keys*
  - *Startup and shutdown of the biometric service*

- *(BIO1030: CAT II) The IAO will ensure only authorized Enrollment Administrators are permitted to create user biometric templates.*

- *(BIO1040: CAT III) The IAO will ensure only authorized Audit Administrators can clear the audit log or modify any of its entries.*

- *(BIO1050: CAT II) The IAO will ensure all Administrators must authenticate to the biometric system to perform administrative functions and that this authentication must include a factor outside of the biometric verification the system supports for ordinary users.*

4.3 Protecting the Enrollment Process

Rapid advances in biometrics will inevitably lead to increasingly accurate and secure biometric technology over time. In this environment, it will become increasingly more difficult for adversaries to breach the verification process and the administrative and cryptographic systems that support it. This means that adversaries are more likely to exploit vulnerabilities in the enrollment process, as this may become the weak link in many biometric implementations.

At its core, the enrollment process establishes a relationship between a user identity and an associated biometric. Consequently, to compromise the enrollment process the attacker may either seek to establish a false identity or to associate an identity with a poor biometric reference template.

4.3.1 Verification of Identification during Enrollment

To guard against the false identity threats, an organization must have a high level of assurance in its identification process. Whenever possible, the enrollment process should be conducted in-person by a trained enrollment administrator who checks for valid photo identification and a request form authorized with a verified signature.

Some biometric systems rely on self-enrollment of biometric data. In this case, there must be strong authentication to the self-enrollment system to ensure that the right person is creating the biometric template. The strength of the enrollment authentication required depends upon the risk profile of the environment being protected with biometrics. In no case, however, should the strength of the authentication required in the enrollment process be less than the strength of authentication required during the verification process because this begs for an attack on the enrollment process. For example, suppose an organization protects access to critical Windows servers with a domain logon and a fingerprint (two-factor authentication). The self-enrollment process, however, is controlled by Windows domain authentication only. In this case, an attacker would try to crack the Windows enrollment authentication in order to enter biometric credentials that subsequently could be used for logon to the critical servers because this would be easier than an attempt to beat the two-factor verification process on the critical servers.

- *(BIO3010: CAT II) The IAO will ensure the enrollment process is conducted by an authorized Enrollment Administrator who will at a minimum check that:*

  - *The enrollee has submitted a completed SAAR DD Form 2875 or similar access authorization form used to authorize access to the system for which the biometric system supports authentication.*

  - *The enrollee is in possession of valid DoD photo identification.*

  - *The photo on this identification matches the physical characteristics of the enrollee.*

- *(BIO3020: CAT I) The IAO will ensure users cannot self-enroll biometric information (i.e., enroll outside of the presence of an authorized Enrollment Administrator).*

4.3.2 Quality Control of the Reference Templates

Even in cases in which the enrollment process provides a high level of assurance that the person submitting biometric credentials is indeed the person whose identity will be associated with the template, there is still a significant risk that the generated template is not an accurate representation of the user. The template submitted may either be too “quiet” or too “noisy”, both of which would allow an adversary to pose as the individual with the poor template. If an enrollee was allowed to speak too softly during enrollment in a voice recognition system, the resultant template would effectively be a recording of silence. If the system were to allow this, then anyone who remained silent during the verification process might be able to pose as the soft-spoken user. The threshold for a match is too low. Similar scenarios apply to other biometrics e.g., poor lighting during enrollment in a facial recognition system might allow null samples during the verification process.

“Quiet” templates may also result when the sample is set to null because the enrollee was unable to supply an adequate sample. Nearly all biometrics are based on the assumption that all enrollees have the associated human characteristic and that it can be captured or measured. In

the DoD environment, many potential enrollees may have lost these physical characteristics as a result of combat in service of their country, which underscores the need to be sensitive to these cases. The appropriate way to handle this situation is to offer an authentication alternative that does not pose an undue burden on the enrollee.

The problem of "noisy" templates is similar to that of the "quiet" template. Significant movement of the subject during enrollment could allow someone to pose as an authorized user by moving suddenly during verification. In these cases, the comparator might accept two blurred samples as a match, when it would have clearly rejected an imposter had the enrollee submitted a more accurate representation of the relevant biometric. Excessive background noise, light or heat during the enrollment process may all introduce a random element into the template that adversaries could exploit at a later time.

If a user has a disability or injury (e.g., a damaged finger or eye) that prevents the generation of a "normal" biometric, then it may be considerably easier to pose as an imposter because there might be a much wider variety of inputs that the biometric system will take as a match for the unusual template. This problem can also occur if the enrollment process is technically flawed. In this case, a "normal" user still may generate a bad template because the capture equipment was not utilized correctly.

To protect against the threat of a poor biometric template, there must be some form of quality control during the initial capture process. Good biometric software will test for the conditions described above and prohibit the creation of clearly inadequately specified templates. Even if this is the case, there is a possibility of a marginal template entering the system (i.e., just good enough to pass quality criteria, but still noisy enough to be susceptible to a sophisticated attack). Whether the biometric software has built-in quality controls or not, the enrollment administrator must be prepared to identify problems with the capture process and re-enroll users who have experienced these problems.

Another related threat is that two people in the system might have a very similar biometric characteristic, which would allow each to pose as the other. In this situation, both individuals may have been enrolled with high quality templates. Therefore, the solution is not to improve the quality of the process. Instead, the enrollment process should include a search through existing templates to determine if there are any matches. This is also a method for discovering whether someone is attempting to enroll twice under two different identities. Fortunately, with most leading biometrics, the probability of two different individuals having the same biometric characteristic is very low, although not impossible. Even identical twins, although they have the same DNA, still have different retina patterns, fingerprints, and hand geometry.

- *(BIO3030: CAT III) The IAO will ensure Enrollment Administrators receive appropriate training that covers, at a minimum:*

  - *The user identification and authorization requirements*
  - *Use of the biometric software and capture device to obtain an acceptable user template*
  - *How to identify when a template is unacceptable and needs to be recreated*

- *(BIO3040: CAT II) Enrollment Administrators will re-create templates when there is an indication that a template has not been properly captured.*

- *(BIO3050: CAT III) The Security Administrator will configure the system to search for matches between the enrolled template and previously existing templates and reject enrollment when a match is discovered. If this process cannot be automated, the Enrollment Administrator will enforce this requirement manually.*

4.3.3 Guarding against Modification of the Reference Templates

If an adversary is able to obtain the digital representation of a user's biometric, the adversary can use it to breach that system or even another one that uses similar technology. If an adversary is able to modify a user's biometric template, then the adversary can grant access to "imposters" by swapping the user's template with that of the imposter.

As mentioned, the storage of biometric templates is often outside the control of the biometric software (e.g., templates on a smart card). For this reason, the *Biometric Verification Mode Protection Profile for Medium Assurance Environments* explicitly excludes template storage from its target of evaluation. Consequently, it is possible for a biometric technology implementation to be based on a Common Criteria validated biometric security product that is appropriately configured, but still have vulnerabilities in its storage component.

- *(BIO4010: CAT II) The Security Administrator will configure the biometric system to encrypt all biometric data resident on non-volatile memory or storage media.*

- *(BIO4015: CAT II) The Security Administrator will ensure biometric templates are protected by operating system permissions.*

- *(BIO4020: CAT II) The Security Administrator will ensure no user ID has access to the files other than those required for running the biometric application software.*

4.4 Protecting the Verification Process

Verification is the process that supports routine user authentication. A user seeking physical or logical entry presents a live biometric sample to a capture device, which extracts a digital representation of the sample and transfers it to a comparator. This section discusses key threats to this process and provides policies which help mitigate these threats.

4.4.1 False Acceptance Rate (FAR) Configuration

The central risk of the verification process is that the technology will mistakenly verify a user's identity when that person is actually someone else – a phenomena known as *false acceptance*. A key goal of many biometric scientists and software developers is to find algorithms that reduce the rate of false acceptances, but a perfect algorithm is essentially unobtainable because human beings are constantly changing (e.g., age, gain/lose weight, sustain injuries, modify behavior). For this reason, the biometric system must have a certain amount of tolerance for error otherwise common changes in individuals would lead to *false rejection.*

The trick is balancing the tradeoff between the *false acceptance rate* (FAR) and *false rejection rate* (FRR). A high FAR means that security may be unacceptably weak. A high FRR means that the technology is likely to be a significant nuisance to falsely rejected users, whose subsequent complaints may undermine the long-term acceptance and therefore viability of the technology.

- *(BIO5010: CAT II) The Biometric Security Administrator will set the FAR to be no greater than 1 in 100,000.*

4.4.2 Anti-Spoofing Techniques

An adversary may present something other than his own biometric to trick the system into verifying someone else's identity, this is known as spoofing. For any biometric, one can devise a potential substitute (spoofing technique) to mimic the real user, though certainly some biometric characteristics and systems are more susceptible to this than others. For facial and iris recognition, spoofing techniques can use of high-resolution still images and/or video. In the case of voice recognition, a tape recording of the valid user's voice may be used to fool the system. Fingerprint capture is included as part of the CAC credentialing process and are expected to be the most used Biometric in DoD. However, there are many techniques for fingerprint spoofing including:

- Breathing on the fingerprint scanner to reactivate the latent fingerprint,
- Using a bag of water on top of the latent fingerprint,
- Dusting the latent fingerprint using graphite powder, stretching adhesive film over it and applying pressure, and
- Using wax casts and silicon molds.

One type of mitigation for anti-spoofing protection is liveness detection. Robust biometric solutions have liveness testing designed to verify that the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. Liveness testing methods range from medically-based measurements like pulse reading, electrocardiogram, lip reading, and body temperature sensing. There are many types of liveness checks, each with an associated level of assurance.

Another solution is to add an attendant to the verification process. However, although supervised access will enhance the security solution, it provides a lower level of assurance and is not an adequate substitute for embedded liveness checks. The attendant could be intentionally or unintentionally distracted, compromised, or forcibly removed. If organizations cannot arrange for an attendant, then they should still perform random spot checks to learn how the biometric technology is used in practice. The mere possibility that human supervision of the verification process might occur on occasion could deter adversaries from attempting to breach the biometric system with a high-quality artifact.

- *(BIO5020: CAT II) The Security Administrator will activate at least one of the available liveness checks.*

4.4.3 Residual Image Check

Another potential attack involves using residual data on the reader or in memory to impersonate someone who authenticated previously. For example, if a valid user leaves his handprint or thumbprint on the capture device, then the next user could possibly submit a blank sample in an attempt to get the capture device to read the residual print that is already on the device.

Similarly, if the attacker gains control of the system, the attacker might be able to use live samples or templates in memory to breach the system. Cryptographic methods such as digital signatures can prevent attackers from inserting or swapping biometric data without detection. If, however, the residual biometric data in memory has already been cryptographically validated, then an attacker may be able to use it to gain entry. Although this would be a sophisticated attack, it is an important one to protect against because of its potential to circumvent cryptographic controls.

Most leading biometric technologies have a means of preventing such an occurrence. The best mechanism is to clear all biometric data from memory before initiating another transaction. Another method is to reject consecutive identical samples. This can be effective because the likelihood that a user would submit the exact same biometric reading is very low and indicative of this type of attack.

- *(BIO5030: CAT II) The Security Administrator will configure the biometric system to prohibit the identical biometric sample from being used in consecutive authentication attempts.*

4.4.4 Limitation on Unsuccessful Authentication Attempts

As with any technical approach to authentication, the likelihood of a security breach is a function of the number of times an attacker can attempt to bypass technical controls. Therefore, one objective of the biometric system configuration is to limit the number of attempts any user can unsuccessfully attempt to authenticate. As with password-based systems, the system should lock the user out and log a security event whenever a user exceeds a certain number of failed logon attempts within a specified timeframe.

When an adversary tries repeated logon attempts, each attempt provides information In some cases, the system may provide more information than a simple yes/no answer. It might also reveal how close a match the credentials supplied is to the ones that would permit access. There is inherent variability in biometric samples and an exact match is often a cause for suspicion. Accordingly, all biometric systems rely on some form of scoring. The issue is who should know the score that results from a sample. While there may be a rationale for the audit administrator to have access to this information, under no circumstances should it be revealed to a user. To do so, would give an attacker clues how to modify inputs to increase the probability of a match.

- *(BIO5040: CAT II) The Security Administrator will configure the biometric system to lock out for 15 minutes any user upon the third unsuccessful authentication attempt within a 15-minute period.*

- *(BIO5050: CAT II) The Security Administrator will configure the biometric system to not reveal to a user any information related to how close the live sample he or she supplies is to the corresponding biometric template.*

4.4.5 Protection against Bypass and Replay

Bypass is when someone circumvents one or more components of the biometric system, most probably the capture device because it is outside the perimeter of the protected system or area. The attacker might compromise the capture hardware or wiring to send electronic or digital representations of biometric data directly to the comparator without first presenting a sample to the capture device. Replay is when someone is able to capture a valid user's biometric data and then use it at a later time for authorized access. The attacker may obtain the biometric data from the stored biometric template or as it is being transmitted from one element of the biometric system to another (e.g., the capture device to the comparator). With the exception of voice recognition systems, replay attacks typically are the follow-on to a successful bypass attack. For example, rather than present a false hand in a hand geometry system, the attacker would learn how someone's hand is translated into an electronic or digital representation of the hand. Then the attacker would bypass the capture device to present the representation to the comparator.

An exact match may be another indication of a replay attack. An exact match occurs when the digital representation of the live sample extracted from the capture device is identical to the stored biometric template to which it is compared. In most applications, an exact match is a good thing, but in biometrics, it is cause for suspicion. There is inherent variability in the sample capture process that makes exact matches unlikely for many biometric technologies. When one occurs, it may indicate that someone has improperly obtained the biometric template and is staging a replay attack.

A potential solution is to reject exact matches, thereby requiring the user to provide another sample. If the user is authorized, then the variability in the sample capture process should lead to something other than an exact match on the second authentication attempt. On the other hand, if the user is an imposter who is in possession of the signed reference template only, then it may be difficult for the imposter to produce a different sample on the second attempt.

Despite the problem associated with exact matches, rejecting them may not be an appropriate strategy. Depending upon the specific capture and extraction technology in place, some biometric solutions may experience considerably more exact matches than others. Rejecting exact matches in these circumstances would be a nuisance. In addition, depending upon the technology, it may be relatively easy for an adversary to enter a small amount of noise in the sample to avoid an exact match but still be close enough for acceptance. In this environment, determining the difference between a true live sample and a replay attack is extremely difficult.

4.5 Fallback and Override Requirements

Fallback is the condition that occurs when the biometric system is not in use. There are three general fallback scenarios: service disruptions; special users (i.e., those unable to present the biometric due to temporary injury or permanent disability); and override of false rejections.

4.5.1 Fallback Procedures

Although biometric systems are expected to be available at all times, a proper implementation of biometrics must consider the case in which the biometric system fails to function. In this case, the system must *fallback* to an authentication alternative. Determined adversaries are likely to study the relative gap between the biometric system and its fallback alternative to determine whether it is easier to breach the biometric system or conduct a denial of service attack on the biometric system and then breach the fallback mechanism.

Consider a case in which a server room is protected by a turnstile that requires a smart card, PIN and retina scan for entry (i.e., three-factor). Under one scenario, fallback might still require the smart card and associated PIN (two-factor). Under another scenario, fallback might involve a manual badge check (single factor with no on-line check for badge revocation). Certainly, the first scenario offers much better protection than the second. If, however, the biometric system was a replacement for the smart card and PIN technology, then there may be no choice for the organization but to implement the manual badge check. Consideration of the fallback contingency is one reason why biometrics should be part of a two-or three-factor solution.

- *(BIO6020: CAT II) The IAO will establish adequate identification and authentication procedures that must be followed whenever the biometric system is unavailable.*

- *(BIO6010: CAT II) The IAO will ensure biometric technology is not the sole means of access control (i.e., it is one component of a two or three-factor authentication solution or it is accompanied by an automated fallback verification system).*

For any given biometric technology, there will be users unable to present the required live biometric sample – people unfortunately lose hands, eyes, the ability to speak, etc. In some cases, the loss of functionality may be temporary – a severe cut on a finger, an eye disease that requires the application of a patch for a period of time, a hand injury that prevents the user from writing or typing as he or she would normally, etc. Unfortunately, any fallback scheme provides a means for an imposter to circumvent the biometric technology. For example, someone with a close resemblance to the user may steal a user's badge and show up with an eye patch or cast to avoid use of the biometric technology that would likely detect the impersonation.

In these situations, the organization must provide some alternative to the biometric system for authentication, but – as with service disruptions, the key is to provide a fallback authentication scheme that still maintains an adequate level of assurance. One method is to introduce a second factor in the authentication process not present in the usual process. For example, if biometrics is coupled with a user name and password, then special users might be allowed to present a token or smart card in lieu of the biometric. Similarly, if biometrics is coupled with a smart card or

token, then the special user might be allowed to enter a password or PIN in lieu of the biometric. If feasible, the authentication should be supervised to guard against improper manipulation.

In some cases, the biometric technology provides partial fallback mechanisms within the system itself. For example, users might enroll both thumbprints and use the right thumbprint for day-to-day verification. If the right thumb is unavailable for any reason, then the user may fallback to the left thumb. These approaches should be employed whenever feasible.

- *(*BIO6030*: CAT II) The IAO will establish adequate written identification and authentication procedures for users that are unable to present the required live biometric sample.*

4.5.2 Override Procedures

Many biometric implementations suffer from a high FRR. When false rejections occur too often, authenticated users are likely to treat any rejection as a false one and override the system to permit access to the rejected individual. This might be something as simple as opening a door for someone who shows a badge and claims that the system is not working. Unfortunately, if an adversary learns of this informal practice, the primary attack strategy is likely to involve a claim of false rejection rather than a more sophisticated approach. When assertions of false rejections become a credible excuse for circumventing the authentication system, biometrics becomes a security threat rather than an enhancement. For this reason, biometric systems must be accurate to be useful.

Inevitably, there will be some false rejections that require intervention to allow proper access (e.g., the recently injured user). Yet the determination of what constitutes a false rejection should not be left to ordinary users.

- *(BIO6040: CAT III) The IAO will designate personnel who have the authority to override false rejections and ensure they receive proper training in how to implement the fallback protocol and verify a user's identity.*

- *(BIO6050: CAT II) The IAO will ensure any override of the biometric system is accompanied by a photo ID check of the user and documentation of the following:*

  - *The name of the user who was granted entry with the override*
  - *The time the override occurred*
  - *The reason for the false rejection*

- *(BIO6060: CAT II) The Biometric Security Administrator will set the FRR to be no greater than 5 in 100.*

4.6 Cryptographic Controls

Proper use of cryptography greatly reduces the risks of several potential vulnerabilities in biometric systems. For example, through the use of digital signatures, the comparator can have

greater assurance that biometric data has not been maliciously modified when it is transferred from storage to the comparator. This risk is substantial because biometric packages may be stored in a location outside the control of the biometric system such as on a smart card or in an on-line user directory.

In this case, encryption might work as follows. During the enrollment process, the biometric system would encrypt and digitally sign any package sent to storage. During the verification process, the comparator would decrypt the package and verify the associated signature to ensure that package was the one created during the enrollment process.

If an adversary gained access to the biometric reference database and managed to replace the biometric data with his own template, then the adversary could impersonate an authorized user. With the application of digital signatures, replacement alone does not suffice for a successful attack because the adversary must also obtain the private key to sign the replaced profile. The security surrounding the key should be greater than that surrounding the biometric package, thereby making this impersonation attack much more difficult to achieve. For instance, the key could be on a hardened server in a secure data center while the biometric template might be on a smart card that could be lost or stolen in any environment.

As with any modern cryptographic system, the security of the system depends upon the keys. The compromise of shared secret or private keys undermines the assurance of anything based on those keys, including – in the case of biometrics – the confidentiality and integrity of biometric templates and live samples, and the non-repudiation of stored biometric packages. In other words, if someone were able to compromise a critical key, that person would probably have the means to bypass the authentication protection that biometrics provides.

- *(BIO2009: CAT II) The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric reference data (using DoD-approved PKI) before it is transmitted from one physical device to another.*

- *(BIO2010: CAT II) The Security Administrator will configure the biometric system uses NIST FIPS 140-2 validated cryptography to implement encryption for communications (data in transit) transmitted from one physical device to another.*

- *(BIO4010: CAT II) The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric reference data resident on non-volatile memory or storage media (data at rest).*

- *(BIO2020: CAT II) The Security Administrator will ensure only the process running biometric software is able to read relevant private or shared secret keys (with the exception of key supercession events during which the Security Administrator may temporarily have the ability to replace the key [e.g., to modify the key file]).*

4.7 Monitoring and Auditing the Biometric System

Auditing for biometrics is as critical as it is for any other information system. Audit logs assist with intrusion detection as well as general troubleshooting. Investigations of information security incidents would be nearly impossible without them.

Ideally, audit systems should be accompanied by an appropriate separation of duties. The security administrator may be able to read the audit log, but should not be able to modify or delete log entries, a role that should be left to an audit administrator. This prevents a malicious security administrator from concealing unauthorized changes to the security configuration or access attempts. If separation of duties is not possible due to resource shortages or organizational structure, then the IAO should ensure that logs are regularly copied to a backup storage medium to which the security administrator does not have write or delete permissions.

In some biometric systems, there may be an option to log a "closeness score" – i.e., a metric that measures the level of similarity between the biometric template and the captured biometric sample. In a proper separation of duties, the security administrator should not be able to view this information because it would provide information on how adjustments to the security parameters might impact the authentication mechanism. For example, if a malicious security administrator could detect that a co-conspirator's biometric had a very close match to another user of the system, then he could adjust the FAR slightly upward to permit the co-conspirator access.

This problem does not arise if the system is configured to log exact matches, but not the quantitative closeness metric. As mentioned, exact matches are evidence of a potential replay attack. In this circumstance, someone may have circumvented the capture device and be transmitting a digital representation of the biometric template. The audit system should record these events in order that this type of behavior may be identified.

It is not feasible to provide specific security guidance for audit log security given the wide variety of potential technologies involved in a biometric deployment. Nevertheless, one can establish a relative standard that requires that biometric audit logs be at least as secure as other logs in that environment.

- *(BIO7010: CAT II) The IAO will ensure the file permissions and storage scheme for biometric audit logs is no less secure than the scheme for the system audit logs of the operating system on which the biometric software resides. The current requirement for audit logs retention is 30 days online and one year offline).*

- *(BIO7020: CAT II) The Security Administrator will configure the biometric system to audit the following transactions:*

  - *All "exact match" verification transactions*
  - *All failed identification or authentication attempts*
  - *All start and stop events for the biometric service*

4.8 Physical Security of the Biometric Components

Physical security is particularly important to biometric systems because the capture device will almost always be outside the boundaries of the area or system to be protected by biometric authentication. Therefore, the trust level of the individuals who can touch and manipulate the capture device is necessarily lower than the trust level of those that the system authenticates. This creates a situation in which less-trusted individuals might be able to tamper with and perhaps bypass the capture device.

One possible strategy to mitigate this risk is to have some form of physical access control *prior* to reaching the capture device. For example, one might have to present a swipe card to enter an anteroom that contains a biometric capture device. Combining two-factor authentication with this form of layered physical security offers a high level of assurance. Another approach is to have human guards monitor the biometric capture device, either directly or through video cameras.

- *(BIO7030: CAT II) The IAO will ensure the physical connections between the following biometric system components are adequately secured.*

  - *The connection between the capture device and the comparator*
  - *The connection between the comparator and the portal*

Adequate security depends upon what is being protected and the risk environment, but it, at a minimum, involves ensuring that no wiring is exposed to unauthenticated users and there is no means of opening the capture device with the use of common tools such as a screwdriver. Requirements for protection of the physical distribution system are found in DoDD 5200. Also see previous section for discussion of a physical intrusion detection system.

5. ACCESS CONTROL INTEGRATION

Protection of DoD restricted and critical assets must follow a layered approach, as described in previous sections. Often, users are asked to present credentials at multiple instances as they encounter various uncontrolled and controlled areas on the way to access resources that may or may not require such protection. Under-protection of an asset may lead to compromise, however, unnecessary over-protection can be inconvenience to the users, costly, and may be detrimental to the desired security posture. Synchronizing and integrating access control mechanisms to recognize vulnerabilities is difficult and some degree of overlap in functionality must be expected. This is done by selectively aggregating access control techniques at the appropriate layer of the security architecture. The access control design or selection team should consider the following general steps when selecting personal authentication methods for the access control solution.

– Step 1: Determine the value of the asset to be protected. This assessment performed by the data owner and is based on mission criticality (MAC Level) and Confidentiality Level (Public, Sensitive, Classified). Determining the value of the asset being protected and the site-specific constraints are the first steps to consider when selecting access control mechanisms as part of a security solution. Value determination is done using the asset's MAC and the results obtained from a thorough risk analysis.

– Step 2: Determine the options available for use as a personal authentication strategy by consulting the access control decision matrices located in subsequent sections. Each table lists the available options based on the highest Confidentiality Level (value) for all assets protected by the access control strategy. Scenarios of this process are provided in a subsequent subsection.

– Step 3: Using the list of available options for protecting the asset (s), the security design team can make decisions about how the various strategies listed could be integrated into the environment based on the following variables.

  - Attended Access. Determine if attended access can or will be used as part of the access control strategy. As the matrices demonstrate, attended access can expand the number of available options significantly; therefore this condition should be integrated into the solution when possible. The security team may need to determine where to place guards and what credentials must be checked to satisfy attended access requirements of the method selected.

  - Residual risk to the Asset. This assessment is based on the results of the risk analysis and recommended mitigation or the team can recommend acceptance of the residual risk based on mission needs.

  - Environmental Considerations: Some strategies cannot be implemented because of tactical, weather, network availability, noise levels, and attendant availability or other constraints as discussed in subsequent sections. Some options consist of several personal authentication methods (e.g., multi-factor combinations). Environmental considerations may require layering of the methods such that not all authentication

proofs are used at the access control point for the asset container layer as discussed in previous sections.

- Technical Requirements: False acceptance and rejection rates, response times, maintenance, encryption, database storage, fallback, backup, frequency of access, and auditing.

- Cost: Procurement costs are impacted by availability on GSA schedule, availability of non-proprietary hardware, software and maintenance costs. Although this document does not directly discuss costs and budget for the access control system, the security selection team should bear in mind that automated solutions such as sensors, remote video, and card readers will increase the cost of the access control solution.

– Step 4: Determine the access control perimeter (outermost point in the environment that access to the asset can and should be controlled), asset container perimeter, and access control point (s). As discussed in previous sections, these may be one or more areas including the facility, building, workspace, or approved asset container. Use all information collected in previous steps to implement the access control solution. The list generated from the matrices provides the team with the minimum authentication requirements for protection at the Asset Container Layer. Selection of access control techniques and methods should be primarily based on asset value and the requirement to mitigate specific risks as determined by the risk assessment. Controls must also implement DoD policy applicable to the mission criticality and confidentiality level of the asset. The implementation may consist of a layered solution but must provide the strongest protection closest to the asset as explained in previous sections.

5.1 Assessing the Value of the Asset

The MAC level indicates the criticality of an asset to the DoD mission based on its purpose and user community. The Confidentiality level of an asset must also be determined and is based on whether the data or resource is restricted or releasable to the public. There are three MAC and three Confidentiality levels. The MAC and Confidentiality Level of the asset is an important factor in determining the security strength the access control solution must provide. MAC and Confidentiality Levels are further defined in Appendix C and DoDI 8500.2. This assessment stage results in a determination of the required level of assurance (LoA) required for the authentication of each transaction for the information system.

5.2 Risk Analysis

The specific access control method selected must also be based upon a risk analysis, which carefully identifies and considers the threats, risks, and costs associated with each solution. OMB Circular A-130, Management of Federal Information Resources, states that agencies must prepare and update a strategy that identifies and mitigates risks associated with each information system. A through risk assessment involves an evaluation of each transaction type and results in the identification of risks and their likelihood of occurrence. When developing or integrating an automated access control system, risk assessment and vulnerability reviews should be integrated into the development lifecycle resulting in a decreased cost for post development remediation.

Failure to conduct a risk analysis could result in implementation of ineffective countermeasures to mitigate vulnerabilities, possibly, leading to loss of protected data, equipment, facilities, or personnel.

The risk analysis should identify potential adversaries and ways of mitigating the threat posed by likely attacks. The adversary of a physical access control system is distinctly different from the adversary of a logical access control system. An adversary attacking a physical access control system must be physically present; therefore the risk of being caught is high. In contrast, an adversary can attack multiple logical access control systems from a remote location.

The Commander or Director will sign the risk analysis, signifying acceptance of any residual risk. The result of the analysis is normally documented in the System Security Authorization Agreement (SSAA) or System Security Plan (SSP). The analysis should be no older than the SSAA but is preferably updated annually.

- *(AC42.010: CAT III) The Security Manager will ensure a risk analysis is conducted and documented for the systems and the facility to be protected.*

- *(AC42.015: CAT III) The Security Manager will ensure unresolved or unmitigated risks (residual risks) are identified, documented, and accepted by the DAA. System changes that are needed to mitigate these residual risks must be documented.*

- *(AC42.020: CAT III) The Security Manager will ensure a security plan is prepared and signed by the commander/director or other appropriately authorized senior management official.*

5.2.1 Compliance Assessment Tools

One method of accessing the site's overall access control posture is to perform a vulnerability analysis using the DISA STIG checklists as a tool for completing a vulnerability self-assessment. This assessment must encompass all of the IT and physical security considerations of the access control and identity management solution within the site's control including, but not limited to the following items supporting the system:

- Access to computer room and office areas
- Assessment of documentation, training, and procedures that support access control
- Network and enclave architecture and component configuration required to support the access control solution
- Directory and authentication device(s) (e.g., Windows domain controllers, RADIUS, etc.)
- Assessment of the access control system application code
- Access control for Web servers
- Access control for Database servers
- Access control for operating system platforms for any of the above

Another method for accessing the site's security posture is to request an SRR by DISA Field Security Operations (FSO). FSO conducts SRRs to provide a minimum level of assurance to

DISA, Joint Commands, and other DoD organizations. Sites may contact the FSO helpdesk for further information and procedures.

The following table highlights some of the relevant STIG checklists and other available tools for obtaining further technology-specific guidance. This is a partial list only. Security teams should consult http://iase.disa.mil/index2.html for additional STIGs when accessing and selecting access control installations and solutions.

Table 5-1. Vulnerability Assessment Checklists and Tools

Checklist Name	Description
Enclave Checklist	Provides guidance on implementing DoD enclave networks.
Traditional (various versions) Checklist	Provides guidance on implementing traditional physical security policy in the IT environment. (STIG and new comprehensive checklist under development)
Network Checklist	Provides security considerations at the network level along with an acceptable level of risks and some guidelines for best network technical practices. Product specific versions available.
Directory Services Checklist.	Where authentication to the database occurs using a directory service, integration between database and directory services must be configured
Secure Remote Computing STIG	Provides the requirements and guidance needed to ensure a secure remote access environment for users within the DoD.
Wireless STIG	Provides guidance on commercial wireless products used by DoD.
Windows (various versions) Security Checklists	Provides requirements for securing IT products with Windows operating system.
Windows Gold Disk	Automated tool used for
UNIX Checklist	Provides requirements for securing IT products with UNIX operating system.
Desktop Application Checklist	Provides technical security policies, requirements, and implementation details for applying security concepts to COTS applications on desktop workstations.
Application Security and Development Checklist	Provides security guidance for use throughout the application development lifecycle. This STIG provides the guidance needed to promote the development, integration, and updating of secure applications.
Database (various versions) Checklist	Provides guidance for configuration of database systems. Security configuration for specific vendor products is provided in the related Database Checklist.

Checklist Name	Description
Windows Gold Disk	Automated tool that assists in securing systems and applications IAW STIG checklists and applicable Center for Internet Security (CIS) benchmarks. Developed to meet the needs of system administrators, Gold Disk supports the ability to detect installed products, identify and remediate applicable vulnerabilities, and generate a file that can be used for asset registration and findings upload into DISA's VMS.
SRR Evaluation Scripts	Database, Unix, Windows and other automated tools for evaluating and securing IT systems IAW STIG checklists.
Network Access Control System	Automated network appliance configured to perform posture assessment and remediation for client systems. Configuration to implement STIG checklists and applicable CIS benchmark compliance.

5.3 Determining the Access Control and Asset Container Perimeters

A multi-disciplined team consisting of the data owner, the IAM, the organization's Physical Security Manager, and the installation, base, or building Physical Security representatives must determine this point of initial control.

Access control systems can be nested within the workspace to limit access to Government assets. For example, sensitive assets may be accessible within the entire workspace perimeter, but classified assets may be stored in a room within the workspace that only a select few are authorized to access. The concept of an internal or nested control point may serve as a perimeter for limited access and special access areas such as classified equipment in computer rooms or open storage areas (cleared for processing classified) where classified equipment and materials cannot be removed. The most stringent personnel authentication challenge should be located nearest the asset being protected, at the asset container layer.

- *(V0007142: CAT I) The IAM and Security Manager will ensure vaults and/or secure rooms for storage of classified material meet the physical security standards of DOD 5200.1-R, Appendix 7.*

- *(V0007145: CAT I) The Security Manager will ensure Classified material and equipment are stored in accordance with its highest classification level or to the level of classified data being processed*

Once the perimeter is determined and established, the IAM and Security Manager will ensure standard Government warning signs or banner messages are displayed identifying the perimeter of area where classified information is processed.

- *(V0007198: CAT II) The areas housing the critical information technology systems are not designated as Restricted Areas.*

5.4 Determining Technical Requirements

Determining the technical requirements of the access control system requires careful evaluation of the technology available to implement the methods selected. Access controls may be as simple as a posted force protection officer granting or denying entry or it may be an automated system that uses authentication technology to control the locking and unlocking of a gate. In many cases, both automated and manual systems are used, where the automated systems support those who routinely work in the protected area and the receptionist or guard supports visitor access processing. As discussed throughout this document, DoD policies for access control implementations mandate capabilities for false acceptance and rejection rates, response times, maintenance, encryption, database access, fallback, backup, and auditing capabilities.

An important consideration is whether the access control point will be attended or unattended. Attended access decreases the capabilities required of the rest of the solution provide added assurance. Attended access control implies that someone other than the individual requesting access permission is present and observing the access attempt. Attended access control will deter an adversary from tampering with the access control system hardware, mounting "brute force" PIN entry attacks, or presentation of artifacts to biometric sensors, for example. DoD has unparalleled strength in force protection and staff vigilance, which can be leveraged to lower the cost of the access control system since these individuals are usually already in place. Unattended access control scenarios may include after hours access or remote access.

Another issue is the environment at the access control point. Weather conditions can adversely affect the equipment and capabilities of reader hardware. The performance of biometric systems with optical sensors (e.g., facial or iris recognition systems and some fingerprint systems) is affected by light variance. Slotted readers used with memory and smart cards may not be well suited for maritime environments because of saline crystallization. Noisy environments on airfields, tactical environments, and lobbies will increase false rejection rates for voice recognition technology.

Network communications is the key to validating digital signatures or conducting biometric comparisons where the biometric reference data is stored in an external database. In many systems, permissions tables must be stored at the access control system because the access control point is not network accessible. For standalone systems, a process for maintaining the database to update revocations and other changes must be part of the technical requirements. Technical requirements must also include the availability of compatible card or biometric readers for network and client devices. Some technologies may not work for these devices because of size or protocol issues. Whenever possible, the security design team should select hardware and software that is Underwriter's Laboratories (UL)-listed and exists on the GSA schedule. Applications and operating systems should not be proprietary and should use standard industry protocols approved for use in DoD.

Special user issues that are unique to the mission may also impact the design. These issues must be considered in the design. The security design team should include a user representative so that these considerations may be captured.

5.5 Integrating Access Control Methods

In most cases, leveraging authentication assurance from different authentication factors offers greater assurance than introducing multiple proofs of the same authentication factor. Verifying *something that you have* and *something that you know* offers greater authentication assurance than verifying possession of multiple things that you have. Furthermore, not all authentication factors offer equivalent authentication assurance. In general, *something that you have* offers less assurance than does *something that you know* or *something that you are*.

DoD policy mandates two- or three-factor authentication as dictated by the level of protection and restrictions required by the asset. As stated in a previous section, FOUO access to MAC II and MAC III assets requires use of no less than two-factor authentication. Classified and/or MAC I assets require the protection of strong two- or three-factor authentication. Although DoD policy is not currently clear regarding the need for three-factor authentication for classified systems, a sound best practice is to combine physical security measures and multi-factor authentication. In this case, a minimum of two factors and an additional instance of the same factor, if correctly implemented, may provide increase assurance. See the following section on Multiple Uses of the Same Authentication Factor for further discussion of this concept. Note that it is possible to achived three-factor authentication using the two-man rule for classified access. That would result in a weak biometric authentication method. However, this is not currently a requirement for all classified access. Ultimately, security protections for an asset are determined by the data owner and specific policies governing the asset type.

To ensure the access control solution meets these policy requirements, the security design or selection team should categorize each method planned for incorporation into the access control architecture as representing *something you have*, *something you know*, or *something you are*. Translating the personal authentication method into the factor will help in determining whether the solution truly represents two- or three-factor authentication. Using this methodology will enable the security design or selection team to see the aggregated protection result of the combined solution. The tables in subsequent subsections list the most commonly used single and multi-factor techniques.

5.5.1 Combining a Hard Token and a PIN

This combination represents *something that you have* and *something that you know*. Its use mitigates the threat of an adversary using a lost or stolen credential to gain access since access requires the individual to swipe the magnetic stripe or bar code of the security hard token (e.g., CAC) and enter a PIN. This combination can be used to support unattended access control for physical access only. In accordance with DoD policy, the CAC cannot be considered as one of the two factors required for access to sensitive logical information.

5.5.2 DoD-approved PKI

Combining a certificate/associated private key and a PIN is the required two-factor authentication mechanism for logical access in DoD. Storing the private key on a hardware token such as the CAC increases the overall assurance of this solution because it is harder for an adversary to acquire the private key.

Access to restricted DoD information systems requires a secure communications channel that is established using a DoD approved communications protocol (e.g., SSL). Authentication is established using digital certificates issued by a DoD approved PKI. Access restrictions are established through an established authorization processes. Remote access to DoD information systems can use this method.

5.5.3 Combining a Hard Token and Biometrics

This combination represents *something that you have* and *something that you are.* Its use mitigates the threat of an adversary using a lost or stolen credential or token but also adds assurance that the person presenting the card for use is the rightful cardholder. This combination of authentication techniques is often used to support a high level of assurance in support of attended or unattended access.

Attended access control can be used in situations that require verification of the CAC using the user's biometric live-capture sample and comparing it to the biometric reference data stored on the CAC. Attended access control will help deter a potential adversary from presenting a fraudulent biometric to the biometric sensor and uses the attendant to verify that the cardholder resembles the photograph printed on the CAC. However, a very sophisticated adversary could produce a fraudulent smart card that verifies the adversary's biometric; consequently, using these procedures would provide equivalent protection to use of a CAC and a PIN discussed previously. The possible flaw in this method is that the verification occurs using the biometric stored on the card.

Unattended access control or higher-level assurance for attended access control can be achieved by requiring verification of the CAC using the user's biometric live-captured sample comparing it to the biometric reference data stored in DEERS database or a local access administrator's database. This verification does not use the biometric data stored on the CAC for verification.

The highest level of assurance that can be achieved using this two-factor combination requires validating the CAC using the user's biometric live-captured sample by comparing it to both locally stored (on card) and remotely stored (off card) biometric reference data.

5.5.4 Combining a PIN and Biometrics

This combination represents *something that you know* and *something that you are.* Its use mitigates the threat of an adversary using a lost or stolen credential and has the added advantage of user convenience (the user does not need to carry anything).

In this scenario the PIN is used much like a Userid. The user enters the PIN and then submits a biometric live-captured sample. The system compares the biometric sample to the biometric reference data associated with the PIN entered (in a one-to-one biometric verification). Alternatively, the user could present a biometric sample to the sensor and the system could conduct a one-to-many biometric identification. The user would be prompted to supply a PIN known by the person that provided the biometric reference data. Note that biometric identification (one-to-many matching) can have performance implications depending on the size

of the biometric database, and biometric verification (one-to-one matching) may be less expensive and provides faster response times.

5.5.5 Three-Factor Authentication

The maximum level of assurance that can be achieved at a single access control point is three-factor authentication which requires integration of techniques representing *something that you have*, *something that you know*, and *something that you are*. A hard token such as the CAC can be used in support of this level of assurance in logical access control as follows:

- DoD-approved PKI keys representing *something that you have.*
- To authenticate an identity by comparing the cardholder to the biometric image stored on and/or in the CAC representing proof of *something that you are.*
- As s*omething that you know* through use of the CAC PIN or the user's knowledge of a password or safe combination.

However, using information stored on the CAC for all three-authentication factors illustrates why integration of access control methods and techniques can itself introduce vulnerabilities. In this scenario, an adversary only needs a valid CAC and a careless, colluding, or coerced user to gain access. Thus, the level of assurance is lessened and this solution is only appropriate for use to protect non-mission critical assets. This vulnerability is especially serious it is placed at the asset container, as it provides the most direct access to the protected asset. To achieve a high level of assurance using three authentication factors, the access control techniques used must be distributed across differing platforms. One solution may be to use the CAC PIN to point to a biometric reference image and a trained force protection officer or guard should be in attendance to verify that a valid CAC user is not being coerced.

5.5.6 Multiple Uses of the Same Authentication Factor

Multiple uses of the same authentication factor represents single-factor authentication regardless of how many methods of the same factor are used in the access control solution. Although this combination may not be used for access to sensitive, classified, or mission critical assets, requiring two uses of *something that you have* (for example, a CAC and a key to a desk drawer) is inherently more secure than using one method only. Requiring two passwords is more secure than requiring one. Requiring personal recognition by colleagues and biometrically verifying your identity (two instantiations of *something that you are*) is more secure than either method alone. Use of this combination, when integrated well, can provided a challenge to the adversary by requiring multiple proofs of authentication for access and thus present multiple barriers to entry.

The least assurance is achieved when two proofs of *something that you have is* implemented. This is because an adversary may be able to steal or find a purse or a briefcase containing multiple authentication devices. Consequently, multiple instances of *something that you have* offer lesser access control assurance than do combinations using multi-factor authentication techniques.

Increased assurance is achieved by using two proofs of *something that you know*. While it may be possible to gain access to a single written password or PIN, it is less likely that more than one password or PIN will be written on a single slip of paper obtained by the adversary. It is possible that an adversary may overcome a user and force them to divulge all of the information required to compromise the security of a system, but this is no greater risk that forcing the authorized user to hand over tokens and divulge passwords or PINs. Consequently, multiple proofs of *something that you know* offer greater assurance than does multiple usages of *something that you have*. However, multiple uses of *something that you know* provide equivalent assurance to a combination of multiple authentication techniques.

The maximum assurance that is achieved by two proofs of the same personal authentication technique would be attended use of *something that you are*. For example, personal recognition by a colleague and passing a biometric verification check can offer a high level of assurance. The highest assurance achieved with this method uses verification of a fingerprint biometric but also either a facial biometric, an iris scan, or hand geometry biometric. This is because the technology or technique required to defeat the security mechanisms of different biometric types are different and involve complex skill sets to duplicate.

5.6 Access Control Decision Matrix

The strongest security controls should be at the point closest to the asset. The access control perimeter is the outermost layer that the data owner and/or Security Manager depends on to ensure access control for the assets being protected. Persons inside the access control perimeter are known or trusted to a certain extent. For example, if the access control perimeter is defined at the building layer, only people authorized for building access should be allowed inside. Exceptions may be handled by providing authorized escorts for visitors. Note that the access control perimeter is not at the same architectural layer for all assets and may be the same as the Asset Container Perimeter. If the asset control perimeter is physically or logically far away from the asset, then controls should be only robust enough to satisfy the data owner and Security Manager since the difficulty of securing such a large space to the level required increases and the strength of the assurance might decrease.

Table 5-1 shows the most commonly used single-factor authentication methods any of which are suitable for use by the access control design team to provide the authentication assurance necessary to protect up to DoD unclassified assets. Note that personal authentication proofing can be distributed across layers depicted in Figure 2-1. This is particularly relevant when designing authentication assurance requirements for systems protecting higher value logical assets, which often leverage both physical access control and logical access control methods across multiple boundaries.

Combinations of the methods in Table 5-1 can be used to protect higher levels of Confidentiality Levels. As discussed in detail throughout Sections 3 and 5, FOUO information requires two-factor authentication and classified information (and MAC I assets) requires three-factor authentication. Thus, the combination should represent the number of factors required to protect the asset based on value (MAC) and Confidentiality Level. Generally, some degree of

redundancy is employed when personal authentication proofing is distributed. The most stringent, trusted authentication proofing should always be closest to the assets being protected.

The methods used in the table will be updated in later versions of this STIG to reflect input from the community, policy changes, and technology advancements. Sample scenarios intended to show how the tables below are used to make access control decisions are included in Appendix D. The information used assumes that a risk analysis has been performed and the environment and value of the asset has been appropriately determined in compliance with DoD policy.

Table 5-2. Personal Authentication Methods

Method	Authentication Factor (s)	Description
Decal	*Something that you have*	Decal mounted onto a motorized vehicle.
Transponder	*Something that you have*	Transponder mounted on a motorized vehicle used for operating an automated entry point.
Badge	*Something that you have*	Not personalized (e.g., visitor badge without name/photo).
Key	*Something that you have*	Physical key of any kind.
Memory Card	*Something that you have*	Refers to memory cards without the PIN, whether personalized or not. (e.g., magnetic stripe, barcode, optical, or smart cards used as memory cards.).
Smart Card	*Something that you have*	Refers to all classes of smart cards, whether personalized or not. Includes cryptographic and non-cryptographic cards. Includes all communications interface types (e.g., contact, contactless, and combi-cards).
Password	*Something that you know*	DoD compliant password or PIN.
Unshared Combination	*Something that you know*	Electronic safe, cipher lock, or PIN pad combination which allows individualized PINS or combinations.
Shared Combination	*Something that you know*	Safe, cipher lock, or PIN pad combination with shared combination.
Colleague Recognition	*Something that you are*	Personal recognition by peers and co-workers. Considered to be attended access. Document policy and train users.
User Recognition	*Something that you are*	Attended access control implementations wherein peers or security guard/personnel perform identification and authentication. Document policy and train users.
Fingerprint Identification	*Something that you are*	Fingerprint authentication, using one- to-many match against templates or images stored in a remote database. This is **not match on card**.
Fingerprint Verification	*Something that you are*	Fingerprint authentication using a one-to-one match against templates or images stored on the CAC biometric reference database.
Hand Geometry	*Something that you are*	Hand Geometry authentication using one-to-many match against templates or images of various characteristics of the hand and finger measurements (not fingerprints) stored in a remote database.
Iris Scan	*Something that you are*	Iris Scan authentication using one-to-many match against templates or images of the eye stored in a remote database.
Digital	*Something that you have*	Issued by DoD-approved PKI. Use of digital signature

Method	Authentication Factor (s)	Description
Certificate	*Something that you know*	with PIN to unlock the private key.
Cryptographic Hardware Token	*Something that you have* *Something that you know*	FIPS 140-2 or NSA certified encryption module used in cryptographic hardware token to implement One time password device and PIN or password solution.
Photo ID	*Something that you have* *Something that you are*	Verified digital or optical photo ID. Use of approved procedures for verifying a non-CAC photo identification card (e.g., drivers' license).
PIV CAC Photo	*Something that you have* *Something that you are*	Procedure for verifying the photo on the CAC.
PIV CAC	*Something you have*	Implies that its presence and validity is verified by an automated system such as a swipe into a reader. The purpose is to validate that this is a valid CAC card only.
	Something that you have *Something that you know*	CAC with PIN for after-hours entry into vacant workspace without after-hours attendant.
	Something that you have *Something that you know* *Something that you are*	Attended or two-person access control using a CAC plus PIN.

APPENDIX A. RELATED PUBLICATIONS

Applicable Policies and Guidelines

Homeland Security Presidential Directive 12 (HSPD 12), Subject: Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.

OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Dec. 16, 2003.

Office of the Secretary of Defense Memorandum, "Common Access Card (CAC) January 2001.

Office of the Secretary of Defense Memorandum, Compliance and Review of Logical Access Control in the Department of Defense (DoD) Processes, 24 January 2007.

NSA Guide to the Secure Configuration and Administration of Oracle9i Database Server, 02 October 2003.

NSA Guide to Secure Configuration and Administration of Microsoft SQL Server 2000, 02 October 2003.

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

NIST FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, February 25, 2005.

NIST Special Publication 800-63, Electronic Authentication Guideline, June 2004.

NIST Special Publication 800-76, Biometric Specification for Personal Identity Verification, February 1, 2006.

DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program, 19 July 2004.

DoD Directive 8500.1, Information Assurance, 24 October 2002.

DoD Directive 8190.3 "Smart Card Technology," 31 August 2002.

DoD Directive 5200.1-R, Information Security Program, January 1997.

DoD Directive 5200.8-R, Physical Security Program, May 1991.

DoD Directive 5230.20, Visits and Assignment of Foreign Representatives, August 12, 1998.

DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, June 16, 1992.

DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 01 April 2004.

DoD Medium Assurance Public Key Infrastructure Registration Authority Reference Certification Practice Statement Addendum – Alternate Login Certificates, 24 July 2006

Global Network Defense Warning Order (Warnord) 06-16 Specified Tasks For Phase 1 Of The Accelerated Public Key Infrastructure (PKI) Implementation, March 2006.

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs), November 2002.

DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, May 2000.

Joint Task Force – Global Network Operations (JTF-GNO) Communications Tasking Order (CTO) 06-02, dated 17 January 2006.

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2, July 30, 2004.

Other References and General Information Sites

Primer on Security Risk Management, White Paper, Innovative Protection Solutions, Draft, May 2007 (Figure 2-1).

http://iase.disa.mil	DISA IASE site
http://www.globalsecurity.org/military/library/policy/army/index.html	Army Field manual
http://csrc.nist.gov/cryptval/	FIPS 140-2 Products lists
http://csrc.nist.gov/npivp/	PIV Validation lists
http://www.tsa.gov/join/business/biometric_qualification.shtm	Transporatation Security Agency (TSA) Qualified Product List (QPL) for biometrics)

APPENDIX B. MISSION ASSURANCE CATEGORIES AND CONFIDENTIALITY LEVELS

Mission Assurance Categories

Mission Assurance Categories (MAC) express the mission criticality and associated characteristics of the application, based on its purpose and user community. DoD has defined three MACs for use in characterization of DoD systems and applications. The application's MAC is a critical factor in determining the strength of the security mechanisms the application must provide. Table C-1 presents the MACs as defined in DoDD 8500.2.

Table B-1. Mission Assurance Categories

Category	Characteristics of Data	Characteristics of Systems
I	1. Vital to operational readiness or mission effectiveness of deployed and contingency forces. 2. Absolutely accurate, timely, available on demand. 3. Classified, sensitive, or unclassified.	National Security Systems (as per Clinger/Cohen Act, Title 10 of the U.S. Code, Section 2.3.10), including systems used to directly perform: – Intelligence activities, – Crypto logic activities related to national security – Command and control of military forces integral to weapon or weapons system – Other system directly critical to military or intelligence missions.
II	1. Important to support of deployed and contingency forces. 2. Absolutely accurate. 3. Can sustain minimal delay without serious effect on operational readiness or mission effectiveness. 4. May be classified but is most likely FOUO or unclassified.	Identified by combatant commands: systems that, if not functional, would preclude the performance of the mission across all operations, including the following. – Readiness – Transport – Sustainment – Modernization – Surveillance/reconnaissance – Finance/contracting – Security – Safety – Health – Information warfare – Information security.
III	1. Necessary to conduct day-to-day business. 2. No material short-term effect on support to deployed/contingency forces. 3. May be classified but is most likely FOUO or unclassified.	Required to perform department-level and component-level core functions.

Confidentiality Levels

In addition to its MAC, another factor in determining an application's security requirements is the sensitivity of the data the application will handle. In DoD, applications handle data of three general hierarchical Confidentiality Levels, with additional gradations/sublevels possible within these Confidentiality Levels as specified in DoD 5200.1-R.

- Classified*:* DoD classifications are Confidential, Secret, Top Secret, and Top Secret /Sensitive Compartmented Information *(*TS/SCI*)*. This data, IA or IA-enable system has been determined, based on appropriate guidance, to require protection against unauthorized disclosure to prevent damage to the national security. Classified data, systems, or applications are highly sensitive and are protected at the most restrictive level of access.

- For Official Use Only (FOUO): This designation is applied to unclassified information that is exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. This data, IA or IA-enable system has been determined, based on appropriate guidance, to require protection (although less restrictive than classified) against unauthorized disclosure.

- Sensitive-But-Unclassified *(SBU):* SBU is Department of State (DOS) original caveat and only they can apply this marking. This caveat should appear in DoD text only when Department of State text is used to support a DoD document. All information that is not intended for public release and is exempt from mandatory public disclosure under the Freedom of Information Act. SBU data and the systems/applications that process SBU data, is protected at the next most restrictive level of access. SBU is afforded the same level of protection as FOUO.

- Public-Releasable*:* Information with release and access that is unrestricted in terms of its confidentiality (although it may have restrictions imposed by the need for information integrity and/or availability). Public-releasable data (and the systems/applications that process public-releasable data) is protected at the least restrictive level of access. Public-releasable data includes Open access and Public access information. Public access would apply to DoD public Web pages that could be read by anyone without first presenting any credentials. By contrast, OPEN access would apply to those Web pages and other resources that require the user to first obtain and present a DoD or acceptable commercial digital certificate, with this certificate being issued to the user's browser.

APPENDIX C. LIST OF ACRONYMS

Acronym	Definition
ACO	Access Card Office
ACP	Access Control Point
BMO	Biometrics Management Office
BSP	Biometric Service Provider
CA	Certificate Authority
CAC	Common Access Card
CIO	Chief Information Officer
COCOM	Combatant Command/Commander
CONOPS	Concept of Operations
CONUS	Continental United States
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-The-Shelf
CPMWG	Certificate Policy Management Working Group
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DBIDS	Defense Biometric Identification System
DCID	Director Central Intelligence Directive
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DMZ	De-militarized Zones
DoD	Department of Defense
DOS	Department of State
EAP	Extensible Authentication Protocol
ECA	External Certificate Authority
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standards
FEDSPEC	Federal Specification
FOUO	For Official Use Only
FRR	False Rejection Rate
FSO	Field Security Operations
GSA	Government Services Agency
HSPD12	Homeland Security Presidential Directive #12
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officers
IASE	Information Assurance Support Environment
ICC	Integrated Circuit Chip
ID	Identification
IDS	Logical Intrusion Detection Systems
ISC	Interagency Security Committee

Acronym	Definition
IPSec	Internet Protocol Security
JTIC	Joint Interoperability Test Command
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
MAC	Media Access Control
N***AC***	National Agency Check
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	Network Security Officer
OS	Operating System
OSD	Office of Secretary of Defense
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PIP	Post Issuance Portal
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program/Project Management Office
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-in User Service
RAPIDS	Real-Time Automated Personnel Identification System
SA	System Administrator
SBU	Sensitive But Unclassified
SM	Security Manager
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDID	Short Description Identifier
SIPRNet	Secret Internet Protocol Router Network
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
NIPRNet	Non-classified (but Sensitive) Internet Protocol
TACACS	Terminal Access Controller Access System
VLAN	Virtual Local Area Networks
VPN	Virtual Private Networks