National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U.S. Government
Wireless Local Area Network (WLAN) Access System Protection Profile
For Basic Robustness Environments

Report Number: CCEVS-VR-06-0026

Dated: 19 May 2006

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validator

Stuart Schaeffer

Aerospace Corporation

El Segundo, California

Common Criteria Testing Laboratory

SAIC

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the evaluation of the U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments. It presents the evaluation results, their justifications, and the conformance results. It acknowledges that the requirements listed in the Protection Profile (PP) are comprehensive and consistent and may be used to develop products whose security targets, which conform to this profile, will satisfy the needs of the sponsoring Government Agency, the National Security Agency (NSA).

The evaluation was performed by the SAIC Common Criteria Testing Laboratory, an accredited Common Criteria Testing Laboratory (CCTL), and was completed in April 2006. The information in this report is largely derived from the PP, provided by NSA, and the Evaluation Technical Report (ETR) written by SAIC. All security functional requirements are derived from Part 2 of the Common Criteria or special explicitly stated requirements using the format of the CC.

Products that are Targets of Evaluation (TOE), addressed by this PP, are network components that provide secure wireless access to a wired or wireless network in an environment that meets the requirements of the Department of Defense (DoD) Basic Robustness Environments. The target robustness level of "basic" is specified in the Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG) and is discussed in Section 1 of the PP. Products that conform to this PP will provide the minimum security requirements for wireless access systems.

The PP addresses the security requirements for an access system, which provides the connection between a (mobile) wireless client device, e.g., a laptop computer with a wireless card installed, and a wired or wireless network and its resources. In a "traditional" wireless LAN, an Access Point (AP) controls the establishment of the link between wireless clients and the wired LAN. An AP is not intended to provide any direct network services to the users that connect through it. The AP relies on the environment in which it resides to assist with WLAN management and provide secure access to the network. Some WLAN access devices may not meet the security requirements stated in this PP by themselves, and it may be necessary for a TOE to include a layered solution, combining additional security components with the AP in order to meet security requirements in this PP. These layered solutions (e.g., VPN, Wireless Gateway, Wireless Security Switch) are all valid as deployment architectures for a wireless access system compliant with this PP.

WLAN access systems must include management capabilities, auditing functions, and authentication to operate in accordance with this PP. To protect the network, the system must address security at Layer 2 (Link Layer) or Layer 3 (Network Layer) or both.

The functionality of a wireless access system may be implemented by more than one physical component. Since an AP does not provide direct network services to the user, it may be one of several components that constitute the access system, or it may be outside the access system, only providing network connectivity to the user. The PP specifies the functional and security requirements for a system as a whole and does not attempt to separate requirements by component. In all cases, wireless traffic must be able to pass to the wired network with the wireless access

system providing the necessary security. The PP also addresses environmental requirements on both the wired network and the wireless access system.

The TOE is required to provide identification and authentication mechanisms for access to services provided by the TOE or to network services mediated by the TOE. This may be done by an authentication server. The origin of the authentication request may be a remote user from the wireless environment, a remote administrative user from the wired environment, or a local administrative user from a TOE console. Administrative users are given the role of "Administrator" and are the only users who have access to the TOE, for installation, configuration, and maintenance.

The TOE includes requirements for cryptographic modules to support policies that require encrypted transmission between the user and the network. Those modules must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-2. Products that currently hold FIPS PUB 140-1 certification are acceptable (conformant with the PP), but only if they were certified prior to the date of adoption of FIPS PUB 140-2. The PP requires the use of Triple DES (3DES) or the Advanced Encryption Standard (AES) as the encryption algorithm.

The TOE must generate audit records, and provide an administrative interface to allow the administrator to select the events that are audited. The PP specifies a minimum set of required auditable events and a minimum list of attributes required in an audit record. Audit records may be stored internally in the TOE or on an external device.

It may be necessary for the TOE to rely on the IT environment to augment the protections offered by the TOE. The PP identifies security objectives for the environment that must be addressed either by assumptions about the environment or by requirements levied on it. Specific requirements for the IT environment are identified in section 5 of the PP.

The use of cryptography and the security functions that may or must be shared between the TOE and the IT environment necessitated some explicit requirements and a number of refinements to existing CC requirements.

The validator monitored the activities of the evaluation team, provided guidance on technical issues and the evaluation processes, and reviewed successive versions of the Protection Profile, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and customer responses. The validator determined that the evaluation showed that the PP satisfies all of the APE security assurance requirements according to the Common Criteria for Information Technology Security Evaluation, Version 2.2 and Part 2 of the Common Methodology for Information Technology Security Evaluation, Version 2.2. Therefore, the validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

The following interpretations applied to this evaluation:

National Interpretations:

I-0412: Configuration Items In The Absence Of Configuration Management

International Interpretations:

CCIMB interpretation 65 - Final Interpretation for RI # 65: No component to call out security function management

The information contained in this Validation Report is not an endorsement of the PP by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product and protection profile evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products or protection profiles desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the protection profile, including:

- The Protection Profile (PP): the fully qualified identifier of the PP as evaluated;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	*U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments*, Version 1.0, April 2006
Evaluation Technical Report	*Evaluation Technical Report For US Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments, Version 0.4*, September 22, 2005
Sponsor	National Security Agency (NSA)
Developer	National Security Agency (NSA)
Evaluators	SAIC
Validator	The Aerospace Corporation

3. SECURITY POLICY

The following security requirements listed in the PP make up the required security policies:

3.1. Administration Policy

Administrators are the only direct users of the TOE and are assumed to be authenticated by the IT environment. Non-administrative users can send data through the TOE but do not have direct access.

The Administration security policy is defined by

- Three iterations of FMT_MOF, to ensure that the administrator has the ability manage the cryptographic, audit, and authentication functions.
- FMT_MSA, to ensure that only secure values are accepted for security attributes, that default values are restrictive, and that administrators may override the default values;
- Three iterations of FMT_MTD, to ensure that only administrators can
    - set rules for selection of events to audit, and
    - create and manage authentication credentials and user identifications;

  and that only users can change their authentication credentials.
- Three iterations of FMT_SMF, to enable administrators to turn encryption on and off, select an encryption algorithm, manage encryption keys, and enable, disable, and query auditing.
- FMT_SMR, to ensure that the TOE supports the roles of administrator and non-administrative wireless user.

3.2.Accountability (Audit) Policy

The Audit security policy calls for the capability to generate audit records for security relevant events and the provision of an administrative interface to allow selection of which events to audit. The policy is defined by

FAU_GEN, requiring audit data generation and association of a user identity with each event recorded;

FAU_SEL, requiring event selection capability

FPY_STM, requiring reliable timestamps.

The PP requires a TOE to generate audit records for the following events:

- Start-up and shutdown of the audit functions;
- Modifications to the audit configuration that occur while the audit collection functions are operating ;
- Changes to the set of rules used to pre-select audit events.
- Use of the authentication mechanism (success or failure);
- Failure to receive a response from the remote authentication server;
- Reaching the threshold for the unsuccessful authentication attempts and the actions taken (e.g. disabling a terminal) and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal);
- Changing the TOE authentication credentials
- Changes to TOE remote authentication settings, to the threshold of failed authentication attempts, and to the session lock timeframe;
- All offered and rejected values for security attributes
- Unsuccessful revocation of security attributes
- Unsuccessful binding of user security attributes to a subject (a process acting on behalf of a user);
- Manual loading of an encryption key;
- Errors detected during cryptographic key transfer;
- Destruction of a cryptographic key;

- Enabling or disabling TOE encryption of wireless traffic;
- Changing the TOE encryption algorithm, including selecting no encryption;
- Initiation/Closure of a trusted communication channel with a remote entity;
- Modifications to the group of users assigned to a role;
- Changes to the time;
- Execution of TOE self test;
- Termination Initiated by the TOE (i.e., the TOE security functions).

The audit requirement specifically prohibits the recording of authentication credentials and failed passwords in audit records.

This list is a mandatory minimum set of events. The PP permits security targets to add additional events.

3.3. Identification and Authentication Policy

The Identification and Authentication (I&A) policy requires the TOE to provide multiple I&A mechanisms for access to services provided by the TOE and to networks and services mediated by the TOE. Administrators must be properly identified and authenticated before performing any administrative tasks. Individual users wishing to communicate via network(s) mediated by the TOE must also be authenticated. The type of authentication mechanism depends on the origin of the authentication request (i.e., remote wireless user, remote administrative user from the network environment, or local administrative user from a TOE console).

Authentication is based on a set of authentication credentials assigned to each user, e.g., a user ID and password. An authentication server (provided by the IT environment) may be used to perform the authentication of both individual network users and remote administrators.

The I&A policy is defined by:

- FIA_AFL, to limit the number of unsuccessful attempts to log in remotely as TOE administrator (in systems where remote administrative login is permitted);
- FIA_ATD, requiring that administrative accounts maintain a password as a security attribute (additional attributes are permitted but not required), and that network user accounts also have associated security attributes (a password is not mandatory);
- FIA_UAU, to limit actions on behalf of locally authenticated users before such users are authenticated;

- FIA_UID, requiring that user authentication be performed before any user actions mediated by the TOE;

- FIA_USB, requiring rules for assigning security attributes to administrative and non-administrative wireless users.

and augmented by an iteration of an explicit requirement:

- FIA_UAU_EXP, to ensure that the TOE provides both local and remote authentication mechanisms and can invoke the remote mechanism at the option of the administrator.

3.4.Encryption (Data Protection) Policy

The data protection policy is defined by:

- FDP_RIP, ensuring data from a packet does not appear in a subsequent packet or in packet data transferred to the TOE's host computer;

- FCS_CKM, creation and destruction of cryptographic keys.

and augmented by explicit requirements:

- FCS_BCM_EXP, implementation and testing of cryptographic modules in conformance with the FIPS 140 cryptographic standard;

- FCS_CKM_EXP, cryptographic key establishment;

- FCS_COP_EXP, random number generation and encryption/decryption operations in conformance with the FIPS 140 cryptographic standard.

- FDP_PUD_EXP, requiring encryption of authenticated user data transmitted to a wireless client and decryption of authenticated user data received from a wireless client when encryption is enabled;

3.5.Self Protection Policy

To ensure that the TOE is functioning correctly:

- FTP_SEP is asserted to require TOE protection of its security domain and separation of the domains of (user) subjects.

and is augmented by explicit requirements:

- FPT_TST_EXP is asserted to require that the TOE

    - run a hardware self-test at start-up and on request;

- run the self-tests of the cryptographic module at start-up and on request;
- run the self-tests of the cryptographic module immediately after generation of a key
- provide a capability to verify the integrity of all TSF data except audit data;
- provide a cryptographic function to verify the integrity of TSF executable code.

- FPT_ITC_EXP is asserted to require that the TOE provide an encrypted communication channel between itself and the TOE IT Environment for authentication, remote logging, and time stamping (and with other IT entities as specified in a security target).

3.6.Session Policy

Wireless user sessions are subject to starting and ending constraints, including the use of a trusted communication path for user authentication. The requirements for this are:

- FTA_TAB, requiring that before establishing a user session, the TOE display an advisory warning message regarding unauthorized use of the TOE.
- FTP_TRP is asserted to require a trusted communication path between the TOE wireless users for authentication of wireless users. The trusted path must have known, trusted endpoints and must protect of data in the channel from modification, replay, and disclosure.
- FTA_SSL is asserted to enable the TOE to terminate a session after a configurable period of user inactivity.

3.7. TOE Security Policy Enforcement (Non-bypassability)

FPT_RVM is asserted to ensure that TOE security policy enforcement functions are invoked and succeed before each function within the TOE Scope of control (TSC) is allowed to proceed.

4. REQUIREMENTS ON THE IT ENVIRONMENT

WLAN Access System TOEs are allowed to rely on the IT environment for supplementation and/or support of the TOE security functions, hence requirements are levied on the Environment to ensure that the TOE and the Environment together meet all security objectives. However, it is acceptable for a security target claiming compliance with this PP to include requirements levied on the Environment by including those requirements as part of the TOE, so long as all security objectives can be shown to be met.

The IT environment is required to include an authentication server, a time server, an audit collection server, and is permitted, but not required, to include a certificate authority. If these servers do not reside on the same physical device as the TOE, their communications with the TOE must be protected.

The IT Environment security requirements are as follows.

4.1. Management

The IT Environment is required to restrict modification of the behavior of Audit, Remote Authentication, and Time Service to the Administrator (in conjunction with the TOE). This is provided by iterations of:

- FMT_MOF, to restrict the ability to modify the behavior of these functions to the administrator;
- FMT_MTD, to restrict the ability to set date and time for timestamps to the administrator;
- FMT_SMR, to maintain an administrator role and associate users with it.

4.2. Audit Policy Support

The Environment is required to support user accountability via audit records, providing protection of the audit trail and support for administrator audit review. This support is provided by:

- FAU_GEN, to associate each auditable event with the identity of the user that caused the event;
- FAU_SAR, to restrict viewing of the audit trail to administrators, to present audit records in a human-readable format, and to search, sort, and reorder audit records.
- FAU_STG, to protect the audit trail from tampering and alert the administrators if the audit trail exceeds a specified amount of storage.

The PP requires the Environment to generate audit records for the following events:

- Unsuccessful attempt to read the audit records
- Any actions taken when audit trail limits are exceeded
- Reaching the threshold for the unsuccessful authentication attempts and the actions taken (e.g. disabling a terminal) and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)
- Use of the authentication mechanism (success or failure)
- Changes to audit server settings
- Changes to authentication server settings
- Changes to time server settings

- Changes to the time data
- Initiation/ or closure of a trusted channel
- Setting of time or date

4.3. Remote User Authentication

The Environment implements a remote user authentication policy defined by:

- FIA_AFL, to limit the number of unsuccessful attempts to log in remotely and prevent the remote user from further authentication attempts until the administrator takes action;
- FIA_ATD, requiring that remotely authenticated users have associated security attributes;
- FIA_UID, requiring remote user authentication and limitation of actions by the environment or the TOE on behalf of a user before authentication;
- FIA_UAU, to limit actions on behalf of remotely authenticated users before such users are authenticated;

and augmented by an iteration of an explicit requirement:

- FIA_UAU_EXP, to require a remote authentication mechanism and authentication by the Environment of a remote user's claimed identity.

4.4. Trusted Channel

An iteration of FTP_ITC_EXP is asserted to ensure the existence of an encrypted channel for communication of authentication data, remote logging data, time and date, and any other IT communication specified in the ST.

4.5. Data Protection

An iteration of FDP_RIP is asserted to ensure that data from one packet does not appear in a subsequent packet or in packet data transferred to the TOE.

4.6. Environment Security Policy Enforcement (Non-bypassability)

An iteration of FPT_RVM is asserted to ensure that security policy enforcement functions of the Environment are invoked and succeed before each function within the Environment's scope of control is allowed to proceed.

4.7. Self Protection

An iteration of FPT_SEP is asserted to require the Environment to protect its security domain and enforce separation of the domains of (user) subjects.

4.8. Reliable Time Stamps

FPT_STM is invoked to ensure that the Environment provides reliable date and time information for the TOE and its own use.

5. ASSUMPTIONS, POLICIES, AND SCOPE

The TOE is not intended to counter two of the threats identified in the Basic Robustness Environment. These two are assumed to be addressed by the environment for the reasons noted below.

Table 1. Basic Robustness Threats not Applicable to the TOE

T.ACCIDENTAL_AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action. Because the storage, retrieval, and review of audit records is provided by the IT environment, and the functional requirements specified in the PP do not provide the functionality required to protect the audit records in the external environment. (The fundamental threat is met by protecting the communication path that the audit records traverse for storage and review.)
T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach. This threat is countered by the FAU_SAA and FAU_ARP requirements, which, because audit review and analysis are functions of the IT environment, were deemed inappropriate for the basic robustness wireless access system TOE and how it is envisioned that it will be administered.

5.1. Usage Assumptions

The TOE is expected to be installed in an IT environment (e.g., PC hardware and O/S) that can address threats and policies outside the capabilities of the TOE and meets the IT environmental requirements necessary to support the correct operation of the TOE.

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.

5.2. Environmental Assumptions

The IT environment is assumed to be capable of providing functionality to counter the threats listed in Table 1. Specifically, it is assumed to provide controlled access to and protection of audit data in storage.

5.3. Clarification of Scope

Products that comply with this PP are considered to be suitable for use in Basic Robustness environments. This PP addresses eleven of the threats in the *Consistency Manual for the Development of U.S. Government Protection Profiles for use in Medium Robustness Environments, Release 3.0*:

Table 2: Threats Countered by the TOE

T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ACCIDENTAL_ CRYPTO_ COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.

T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.

The PP addresses the three security policies in the Basic Robustness Environment augmented by three other policies:

Table 3: Organizational Security Policies Addressed by the TOE

Basic Robustness Policies	
P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY_VALIDATED (Identical to P.CRYPTOGRAPHY in the Consistency Guide)	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
Policies Specific To This PP	
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

6. ARCHITECTURAL INFORMATION

A wireless local area network (WLAN) is a network in which network nodes communicate by broadcasting wireless (radiated) signals rather than a physical wired connection. Client devices transmits and receive signals to and from another network node via a wireless access system, which provides the connection between a (mobile) wireless client device and a wired or wireless network. The connection is made through an Access Point (AP).

An access system may contain an AP, or the AP may be separate network component. The function of the access system is to provide

- management capabilities,
- authentication
- auditing functions, not including storage and review capabilities, which are relegated to the IT environment, and
- encryption and decryption of network traffic.

Wireless clients are generally easily carried about and used in public spaces, and even in restricted operational environments their signals might be detected by unauthorized equipment. In order to maintain confidentially of transmissions, encryption is essential. For much government

use, trusted strong encryption is needed, and this PP requires the use of FIPS certified encryption software.

7. DOCUMENTATION

No external supporting documentation was used in the evaluation.

8. RESULTS OF THE EVALUATION

The U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile For Basic Robustness Environments has satisfied the evaluation requirements of the APE section of the CEM. The PP was assessed against the protection profile requirements as stated in the Common Criteria for Information Technology Security Evaluation Version 2.2.

9. VALIDATOR COMMENTS

None.

10. LIST OF ACRONYMS

CC	Common Criteria
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
ISSE	Information System Security Engineers
IT	Information Technology
OSP	Organization Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RF	Radio Frequency
SF	Security Function
SFP	Security Function Policy

11. BIBLIOGRAPHY

[1] Consistency Instruction Manual For development of US Government Protection Profiles For use in Basic Robustness Environments

[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2 Revision 256.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2 Revision 256.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2 Revision 256.

[6] Evaluation Methodology ASE/APE Trial Use Version, Version 2.4, March 2004, Revision 256, CCIMB-2004-03-004

[7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/001

[8] FIPS PUB 140-2:Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001.

[9] Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance,16 June 2000