National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Department of Defense Public Key Infrastructure And Key Management Infrastructure Token Protection Profile (Medium Robustness) Version 3.0

Report Number: **CCEVS-VR-02-0017**
Dated: **27 March 2002**
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

Validation Team

Donald Phillips
Meg Weinberg
Mitretek Systems Inc.,
Falls Church, VA

Common Criteria Testing Laboratory

Computer Sciences Corporation
Annapolis Junction, MD

Table of Contents

Executive Summary

An evaluation of the Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness) [DoD PKI Token PP] Final, Version 3.0, 22 March 2002. The [DoD PKI Token PP] Protection Profile evaluation commenced on August 9, 2001 and was completed on 27 March 2002. The [DoD PKI Token PP] evaluation was performed by Computer Sciences Corporation in the United States. The evaluation was conducted in accordance with the requirements drawn from the Common Criteria CCv2.1, Part 3, Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the [DoD PKI Token PP] contains realistic security objectives that are countered by stated threats. The CC class also offers confidence that the Protection Profile is internally consistent, coherent and technically sound.

Computer Sciences Corporation, the Common Criteria Testing Laboratory [CCTL], is certified by the NIAP validation body for laboratory accreditation. The CCTL has presented CEM work units and rationale that are consistent with the CC [Common Criteria], the CEM [The Common Evaluation Methodology] and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories. The CCTL team concluded that the requirements of the APE class have been met. Therefore, a **pass** verdict has been issued, by the CCTL, for the protection profile assurance family.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, The Common Evaluation Methodology [CEM], and CCEVS.

Evaluation Details

Dates of Evaluation: 9 August 2001 – 27 March 2002
Evaluated Product: Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness) Version 3.0 22 March 2002
Developer: Booz-Allen & Hamilton Inc., National Security Agency, 9800 Savage Road, Fort George G. Meade, MD 20755-6000
CCTL: Computer Sciences Corporation, 132 National Business Parkway, Annapolis Junction, MD 20701
Validation Team: Donald W. Phillips, Meg Weinberg, Mitretek Systems Inc., Falls Church, VA
Evaluation Class: EAL4 augmented with ALC_TAT.3 and AVA_VLA.3

Protection Profile Identification

Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness) Version 3.0 22 dated 22 March 2002.

Protection Profile Overview

This [DoD PKI Token] PP specifies the information technology (IT) security requirements for a token to be used with sensitive but unclassified (SBU) applications (Class 4) in the DoD Public Key Infrastructure (PKI) and the Key Management Infrastructure (KMI). The Key Management Infrastructure's purpose is to unify existing and planned key management systems with the DoD PKI to create a single, integrated whole. Due to the relationship between KMI and the DoD PKI, this protection profile specifies the security requirements for a token that will be used by both infrastructures. Tokens conformant to this PP provide adequate security services, mechanisms, and assurances to process sensitive information in medium robustness environments, as specified in the "Guidance and Policy for Department of Defense Information Assurance" (GiG). Medium robustness is defined as having a classification of SBU (DoD Unclassified), an Evalution Assurance Level (EAL) of 4+, and an encryption requirement of FIPS 140-2 Level 2 for Subscribers/Level3 for Registration Authorities and Certificate Authorities. The services provided by the DoD PKI and KMI include the generation, distribution, control, tracking, and destruction of public key certificates. The primary goal of the DoD PKI and KMI is to securely transport sensitive but unclassified or unclassified information using unprotected networks. The DoD PKI and KMI token carries public key certificates used to authenticate its user in public key transactions and applications.

The security requirements in this PP apply to the DoD PKI and KMI token as issued to the token holder. These requirements cover the token's integrated circuit, operating software, and specific applications when processing DoD information. This PP does not cover security requirements for token terminals or networks interfacing with them. Throughout the requirements section in this protection profile, references are made to requirements for FIPS 140-2 Level 2 for Subscribers/Level 3 for Registration Authorities and Certificate Authorities. If the DoD Common Access Card (CAC) issuing infrastructure is not capable of issuing two different levels of cards, then all CACs will be required to meet FIPS 140-2 Level 3.

Appendix A lists references, and Appendices B and C, respectively, list acronyms and a glossary of terms used in this PP.

Interpretations

None

Threats

Listed below are specific threats to IT security that should be countered by the [DoD PKI Token PP]:

Physical Attack

T.E_Manip: Electrical Manipulation of the IC	An attacker may utilize electrical probing and manipulating of the TOE to modify security-critical data so that the TOE can be used fraudulently.
T.P_Modify: Physical Modification of the IC	An attacker my physically modify the TOE in order to reveal design – or security-related information.
T.P_Probe: Physical Probing of the IC	An attacker may perform physical probing of the TOE to reveal design information and operational contents.
T.Power_Clock: Power and Clock	An attacker may interrupt, reset, or alter TOE power or clock to disrupt security critical functions.

Logical Attack

T.Bad_Load: Load Bad Software or Security Data	An attacker, an SSO, or the user may load improper software (operating system, executable files) or security data (authentication information, keys, access control information) onto the TOE that could modify or expose software (e.g., security functions) or data on the TOE.
T.Component_Fail: Failure of a Critical System	An attacker exploits a failure of one or more system components, resulting in the loss of system-critical functionality.
T.Developer_Flawed_Code: Software containing security-related flaws	An attacker exploits code delivered by a system or application developer that does not perform according to specifications, contains security flaws, or is not appropriate for operational use.
T.Flt_Ins: Insertion of Faults	An attacker may determine security-critical information through observation of the results of repetitive insertion of selected data.
T.Forced_State_Change: Forced State Change	An attacker may force the TOE into a nonsecure state through inappropriate termination of selected operations.
T.Inv_Inp: Invalid Input	An attacker or authorized user of the TOE may compromise the security features of the TOE through the introduction of invalid inputs.
T.Spoof: Spoofing Legitimate System Services	An attacker tricks users into interacting with spurious system services, e.g., an unauthorized (bogus) terminal, that request sensitive information from the TOE.
T.UA_Use: Unauthorized Program Use	An attacker may utilize unauthorized programs to penetrate or modify the security functions of the TOE.

Access Control

T.First_Use: Fraud on First Use	An attacker may gain access to TOE information by unauthorized use of a new, previously unissued TOE.
T.Impers: Impersonation	An attacker may gain access to TOE information by impersonating an authorized user of the TOE.

Unanticipated Interactions

T.App_Ftn: Use of Unallowed Application Functions	An attacker may exploit interactions between applications to expose sensitive TOE or user data.
T.Fail_Secure: Failing in a Nonsecure State	An attacker may cause failure of the TOE security functions by exposing the TOE to conditions outside of its normal operating range, causing the TOE to enter a non-secure state.
T.LC_Ftn: Use of Unallowed Life-Cycle Functions	An attacker may exploit interactions between life-cycle functions to expose sensitive TOE or user data.
T.Res_Con: Resource Contention	A user or attacker may willfully, or through negligence, monopolize resources of the TOE, denying service to another user or function.

Cryptography

T.Crypt_Attk: Cryptographic Attack	An attacker may defeat security functions through a cryptographic attack against the algorithm, through cryptanalysis on encrypted data, or through a brute-force attack.

Information Monitoring

T.Hacker_Comm_Eavesdrop: Hacker Eavesdrop on User Data Communications	Hacker obtains user data by eavesdropping on communications lines.
T.I_Leak: Information Leak	An attacker may exploit information that is leaked from the TOE during normal usage.
T.Link: Linkage of Multiple Observations	An attacker may observe multiple uses of resources or services and, by linking these observations, deduce information that would reveal critical security information.

Miscellaneous Threats

T.Clon: Cloning	An attacker may clone part or all of a functional TOE to develop further attacks.
T.Env_Strs: Environmental Stress	An attacker may exploit failures in the TOE induced by environmental stress.
T.Lnk_Att: Linked Attacked	An attacker may perform successive attacks with the result that the TOE becomes unstable or some aspect of the security functionality is degraded. A following attack may then be successfully executed.

T.Rep_Atk: Repetitive Attack	An attacker may utilize repetitive, undetected attempts at penetration to expose memory contents or to change security-critical elements in the TOE.

Operating Environment

T.Hacker_Social_Engineer: Social Engineering	A hacker uses social engineering techniques to gain information about system entry, use, design, or operation.
T.Privilege: Abuse by Privileged Users	A careless, willfully negligent, or hostile administrator or other privileged user may create a compromise of the TOE assets through execution of actions that expose, change, or destroy the security functions or the protected/security-critical data.

Security Policy

Policy statements whose enforcement must be provided by the [DoD PKI Token PP] security mechanisms:

P.Key_Length: Cryptographic Key Length	X.509 Certificate Policy for the U.S. Department of Defense. Digital Signature Standard keys shall use at least 160 bit private key and at least 1024 bit prime modulus. Minimum public key size shall be 1024 bits for Key Exchange Algorithm (KEA). Minumum public key size shall be 2048 bits for RSA. For Class 4, Elliptic Curve Digital Signature Algorithm key prime field (//p//) shall be not less than 384 bits.
P.Protection_Mechanisms: Application of Protection Mechanisms	DoD Information Assurance Guidance and Policy Memorandum 6-8510. Protection mechanisms shall be applied such that the TOE maintains the appropriate level of confidentiality, integrity, authentication, and nonrepudiation based on mission criticality, sensitivity of information handled by the system, and need to know.

Usage Assumptions

This protection profile specifies the following usage assumptions for the TOE:

A.Dev_Protect: Protection of TOE by Developer	During the development and manufacturing process, the TOE and associated development tools are assumed to be protected by the developer from any kind of unauthorized use, e.g., tampering or theft.
A.Key_Gen: Key Exchange Key Generation	Key exchange keys are assumed to be generated off-TOE in a secure manner in accordance with X.509 Certificate Policy.
A.Secure_Host_Comms: Secure Host Communications	If the host establishes a secure connection between it and the TOE that conforms to the requirements imposed by the TOE, the host including code and security data it contains, is assumed to be trusted.

Security Content of PP

- Cryptographic Support employing cryptographic functionality and addressing key management and operational use of cryptographic keys.
- User Data Protection relating to the subset and security attribute(s) based access control, basic data authentication, import/export of user data without security attributes, information flow control, internal transfer protection, and residual information protection.
- Identification and Authentication supporting PKI Token access control function policies to identify person and/or entity performing PKI Token functions.
- Security Management covering aspects of management of security functions including management of behavior, security attributes, secure security attributes, static attribute initialization, management of TSF data and TSF limits, management of secure TSF data, revocation of security attributes, and management of assuming and restricting roles.
- Protection of the TOE Security Functions supporting the functions that manage and protect the integrity of confidential TSF data from disclosure and modification through the use of environment failure, abstract machine testing, management of network traffic of TSF data from remote hosts or data transmitted from separate parts of the TOE, detection and resistance from physical attack, recovery failure, non-bybassability, and domain separation.
- Resource Utilization is achieved by imposing quotas on the following resources that include, memory, program space and individual users or groups over a specified time.
- Trusted Path/Channels providing protection from modification and disclosure of transmitted data by means of a secure communications path between the TOE and local and remote users.

Assurance Content of PP

The [DoD PKI Token PP] provides for Assurance at the EAL 4 – augmented level with assurance components as shown in the table below:

EAL4 Augmented Assurance Requirements

Assurance Class	**Assurance Family**
Configuration Management	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
Delivery and operation	ADO_DEL.2 ADO_IGS.1
Development	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1

	ADV_RCR.1 ADV_SPM.1
Guidance documents	AGD_ADM.1 AGD_USR.1
Life cycle support	ALC_DVS.1 ALC_LCD.1 **ALC_TAT.3 augmented**
Test	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
Vulnerability assessment	AVA_MSU.2 AVA_SOF.1 **AVA_VLA.3 augmented**

Documentation

The evidence used in this evaluation is based solely upon:

[DoD PKI Token PP] Profile (Department of Defense Public Key Infrastructure Token Protection Profile) Final, Version 3.0 December xx, 2001 (and previous versions leading up to this document).

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

Results of the Evaluation

The Common Criteria Testing Laboratory [CCTL] team conducted the evaluation according to the CC and the CEM and concluded that the requirements of the APE class were met. Therefore, a **pass** verdict has been issued for the protection profile assurance family.

Validator Comments/Recommendations

The Validation team observed that the evaluation and all of its activities were in accordance with the CC, the CEM, and CCEVS practices. The Validator agrees that the CCTL presented appropriate CEM work units and rationale to support a **pass** verdict. The validation team therefore concludes that the evaluation, and results of **pass** for the Department of Defense Public key Infrastructure Token Protection Profile (Medium Robustness) Version 3.0, is complete and correct. The validation team recommends that this evaluation be approved by the CCEVS.