National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

U. S. Government Protection Profile Authorization Server For Basic Robustness Environments, Version 1.0

Report Number:	**CCEVS-VR-05-0106**
Dated:	**29 June 2005**
Version:	**1.01**

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
Kathy Cunningham
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team
Science Applications International Corporation (SAIC)
7124 Gateway Drive
Columbia, MD 21046

Table of Contents

1. Executive Summary

The evaluation of the U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0 was performed by SAIC CCTL in the United States and was completed on 29 June 2005. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation for conformance to the APE requirements of the Common Criteria for IT Security Evaluation. Trial version 2.4 of the APE requirements and methodology were used for the evaluation of the PP, while the security functional requirements and security assurance requirements included within the PP are from version 2.2 of the CC/CEM.

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The information contained in this Validation Report is not an endorsement of the U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, version 1.0 by any agency of the US Government and no warranty of the PP is either expressed or implied.

The SAIC evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0, Dated June 22, 2005 produced by U.S Government and the Evaluation Technical Report (ETR) for U.S Government Protection Profile Authorization Server for Basic Robustness Environments, Dated June 29, 2005, produced by SAIC.

1.1 Evaluation Details

Dates of Evaluation: October 2004 through June 2005

Evaluated Product: U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0, dated June 22, 2005

Developer: National Security Agency (NSA)

CCTL: SAIC, Columbia, MD

Validation Team: Kathy Cunningham, National Security Agency, Ft. Meade, MD

Evaluation Class: None

PP Conformance: None

1.2 Interpretations

The evaluation team determined that the following National Interpretations were applicable to this evaluation:

I-0407	Empty Selections Or Assignments, 2003-08-21
I-0410	Auditing of Subject Identity For Unsuccessful Logins, 2002-01-04
I-0415	User Attributes to be Bound should be Specified, 2002-03-04
I-0425	Settable Failure Limits Are Permitted, 2002-12-05
I-0429	Selecting One Or More, 2003-08-12

1.3 Threats to Security

The Protection Profile identified the following Threats:

T.ACCIDENTAL_ADMIN_ ERROR: An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.ACCIDENTAL_AUDIT_ COMPROMISE: An administrative 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.

T.ACCIDENTAL_CRYPTO_ COMPROMISE: An administrative 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.LOW_PRIORITY: A low priority process may exhaust resources required by the TOE.

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: Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.

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: An attacking 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 the data for which they are not authorized according to the TOE security policy.

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.

2. Identification

2.1 PP and TOE Identification

PP: U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0, dated June 22, 2005.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Evaluation Methodology ASE/APE Trial Use Version, Version 2.4, Revision 256, March 2004

2.2 PP Overview

The "U.S. Government Protection Profile Authorization Server for Basic Robustness Environments" specifies a set of security functional and assurance requirements for Authorization Server products. The Authorization Server is a family of software products that supports access control of IT resources (e.g., web servers, databases, application servers, individual web pages, and specific data files/objects). Access control, or authorization, is defined as determining whether a *principal* shall be granted permission to perform an *operation* on a *resource*. The term *principal* indicates an authenticated identity, and might be a user at a web browser, web service, or other application. The *operation* would most often be read access (e.g. viewing a web page or querying a web service interface), but might also include other operations such as creation, modification and deletion. The *resource* could be static content (e.g., web pages, files and images) or dynamic (e.g., web applications and services).

Authorization Server functionality provides a capability to map a principal's identity to a set of privilege attributes. It also provides a mechanism to assign access requirements for IT resources. When acting as an Authorization Server, the TOE executes pre-defined rules or policies which compare a principal's privilege attributes to the requested IT resources access requirements to make an access control decision. The majority of products with PPASBRE compliant STs will support Authorization Server functionality, but it is not mandatory (it is possible to comply with PPASBRE with only Attribute Authority functionality).

Additional functionality may or may not be present in an Authorization Server product and will be specified with refinements of the security functional requirements (SFRs) by the ST author – relevant SFRs and application notes in the relevant SFRs will detail where refinements should be applied. The additional functionality includes:

- Authorization Enforcement – If the TOE enforces the access control decision to grant or deny access to a resource.
- Authentication Server – If the TOE performs authentication of the principals who are attempting to access protected resources.
- Attribute Authority – If the TOE provides an interface for external applications and/or users to obtain principals' privilege attributes.

The deployment of Authorization Servers can also be characterized as a deployment of "Privilege Management Infrastructure" (PMI). The PMI can be defined as the systems, processes and software required to operate an "Authorization Service."

PPASBRE-conformant products provide the ability to protect themselves and their associated data from unauthorized access or modification while ensuring accountability for authorized actions.

The PPASBRE is a "software only" PP dependent on the IT environment (hardware, operating system, and other software products) to meet some of the security functional requirements for a Basic Robustness environment (as defined by the NSA Information Assurance Directorate (IAD) document "Protection Profile (PP) Consistency Guidance for Basic Robustness"). This protection profile provides a level of protection that is appropriate for IT environments that have main Authorization Server components on a private protected network (e.g., behind firewalls) and administered by highly trusted users. The TOE and IT Environment do not fully address threats posed by malicious administrative or system development personnel. PPASBRE-conformant products are suitable for use in both commercial and government environments.

The PPASBRE was constructed to provide a target and metric for the development of Authorization Server software. This PP identifies security functions and assurances representative of the lowest common set of requirements that should be addressed by a useful Authorization Server. Targets of Evaluation (TOEs) compliant with this PP must meet the assurance requirements of Evaluation Assurance Level (EAL) 2 augmented.

This PP defines:

- Assumptions about the security aspects of the environment in which the TOE will be used;
- Threats that are to be addressed by the TOE;
- Organizational Security Policies pertaining to the TOE;
- Security Objectives of the TOE and its environment;
- Functional and Assurance Requirements to meet those security objectives; and
- Rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

A TOE conformant to this PP satisfies the specified functional requirements, as well as the Basic Robustness assurance requirements. The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 2 requirements augmented from part 3 of the Common Criteria with Informal TOE Security Policy Model (ADV_SPM.1), Flaw Remediation (ALC_FLR.2), Misuse-Examination Guidance (AVA_MSU.1) and Analysis of Coverage (ATE_COV.2).

These augmented assurance requirements were deemed necessary by NSA to reduce the ambiguity in the associated CC assurance families and to provide the level of assurance appropriate for basic robustness environments. For more detail information on the assurance requirements, reference Section 5.3 of this PP.

2.2.1 Relate Protection Profiles

There are no PPs that directly relate to the Authorization Server software. However, the following PPs provide security requirements to components that make up the IT Environment in which the Authorization Server software is deployed:

- Web: Web Server Protection Profile, Web Browser Protection Profile Draft, Version: .6, dated 31 July 2001

  If the TOE supports remote administration via web browser, then the guidance documents shall instruct administrators to use a web browser that has been evaluated to be compliant with the Web Server Protection Profile (if any such web browsers exist at the time of the TOE evaluation).

- Operating Systems: Controlled Access (Basic Robustness/C2) (CAPP) Version. 1.d, dated 8 October 1988

  The TOE shall run on an operating system that has been evaluated to be compliant with the Controlled Access Protection Profile.

2.3 IT Security Environment

The TOE described in this PP is intended to operate in environments having a basic level of robustness.

A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE

Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimum. Authorized users of the TOE are cleared for all information managed by the Authorization Server, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low.

Entities in the IT environment on which the TOE depends for security functions must be of at least the same level of robustness as the TOE.

3. Security Policy

The Operational Security Policies defined for the TOE:

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

P.ACCOUNTABILITY: The TOE shall log all actions by authorized users such that the authorized users can be held accountable for their actions within the TOE.

P.BASIC_ROBUSTNESS: The TOE must be developed in accordance with the Basic Robustness guidelines.

P.CAPP_OS: The operating system the TOE operates on top of must be evaluated to be compliant with the Controlled Access Protection Profile.

P.COMMS: Communications exist between the TOE components (internally) and between the TOE components and the IT components.

P.CRYPTOGRAPHY: Only NIST FIPS 140-2 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).

P.HIGH_AVAILABILITY: The TOE shall include providing resource allocations to support priority of service and fault tolerance.

P.NO_GENERAL_PURPOSE: There will be no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the hardware platforms that the TOE administrative and authorization policy engine software are installed. If Authorization Server "Agent" software is part of the TOE, then the system on which the Agent operates is exempt from this assumption.

P.TOE_ENVIRONMENT_ACCESS: The TOE environment will provide mechanisms that control a user's logical access to the TOE environmental components.

P.WEB_BROWSER_PP: If administrators use a web browser to access the TOE for remote administration, they must to use software that has been evaluated to the Web Browser Protection Profile.

4. Assumptions

Personnel and Physical Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

A.IT_ACCESS: The TOE has access to all the IT System data it needs to perform its functions.

A.LOWEXP: The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

A.MANAGE: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

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

A.NO_TOE_BYPASS: Principals cannot gain access to resources protected by the TOE without passing through the TOE access control mechanisms.

A.PHYSICAL: The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.SCALABLE: The TOE environment is appropriately scalable to provide support to the IT Systems in the organization it is deployed.

5. Architectural Information

This PP specifies the minimum security requirements for a TOE composed of several "software only" components, which together, make up an Authorization Server system. The purpose of an

Authorization Server is to provide an organization with a web access management solution that helps to enable secure access to web-based resources. These commercial security products enhance website security management by providing a platform for centrally managing access to all web resources and applications. In a large organization, this is cost saving over building proprietary user directories and access control systems in the individual applications. The authorization policy management feature of these products enables central or distributed management of user access privileges. The products also provide for the creation of business or policy rules, often called rulesets, which can incorporate both static (such as a role) or dynamic attributes (such as a principal's checking account balance) to define the access control requirements to protect web-based resources (e.g.: Universal Resource Locators (URLs), files, and objects).

Authorization Server products often also provide an enforcement functionality in the form of either an "agent" which provides the access control decision enforcement point for application servers or by sitting as a proxy in front of the application server.

In addition to web and application server access management, Authorization Server software products may provide an API to enable applications to make their own access control decisions by obtaining a principal's privilege attributes. In this mode of operation, the Authorization Server software functions as an "Attribute Authority".

An Authorization Server requires an authenticated identity as an input to the access control decision. In the core configuration the Authorization Server obtains the authenticated identity as an input, but some products will perform the authentication themselves, in which case the server functions also as an "Authentication Server" providing a Single Sign-on (SSO) capability that allows principals to navigate across web-based resources, both within a single site and across multiple sites, while authenticating only once.

The following components make up an Authorization Server. Not all component functionality will necessarily, be supported by every Authorization Server product. The Authorization Server Component Table summarizes the Authorization Server components and indicates which are mandatory and which are optional. Usage Scenarios of how the different components can be combined are found in section 2.2 of the PP.

Authorization Server Components Table

COMPONENT	REQUIREMENT
Administrative User Interface	Mandatory
Privilege Attribute Data Store	Mandatory
Access Policy Data Store	Mandatory
Authorization Server Policy Decision Engine	Required if Access Control Decision API, Authorization Enforcement Engine, or Authorization Enforcement Agent is present.
Access Control Decision API	At least one of these four components must be present.
Authorization Enforcement Engine	
Authorization Enforcement Agent	

Attribute Authority	
Authentication Server	Optional

Administrative User Interface capabilities, allows administrators to securely log on and gain access to the TOE's management tools. Administrators may gain access to this component either via a web based interface or a client/server interface, depending on the product's design. If the web interface is used, the administrator's browser should be required to meet the security requirements outlined in the "Web Browser Protection Profile." If a client program is used, the client software is part of the TOE.

Privilege Attribute Data Store (PADS) contains data about the principal that make up the authorization domain. This data always includes the privilege attributes that are used by the policy decision engine to make the access control decision. Additionally, if the authentication server functionality is included, the PADS data may include additional information required to authenticate the user, for example password information.

This component also provides the tools to create and modify privilege attributes or entitlements, including creating and managing groups as well as changing values for existing attributes.

Access Policy Data Store contains the data that defines the access control policy. Each policy defines who can access each resource, the conditions under which access will be allowed, and the privilege attribute information needed for a successful authorization.

This software component provides the tools to manage the policy information as well as the storage thereof.

Authorization Server Policy Decision Engine provides a mapping between the required access criteria for a web based resource and privilege attributes. It performs the required computation to make an access control decision. This component, which would reside in a protected enclave, would require secure interfaces to the agent and to the data stores to obtain the information needed to make the policy decision.

Access Control Decision API is generally provided by Authorization Server software products. The API allows authorized applications to obtain access control decisions from the Authorization Server's policy engine. In the cases in which the Authorization Server does not perform Authorization Enforcement, this interface is required for applications to determine whether to grant or deny access to the requested resources.

This API accepts an authenticated principal, the requested resource, and the requested operation as input. The API would then access the privilege attribute and policy data stores as necessary to make the decision, and the Policy Engine would then make the decision and the API would return a "Grant or Deny" response to the requesting software application.

Authorization Enforcement Engine controls the resources and enforces the access control decisions. The enforcement engine can be implemented through the Authorization Enforcement Agent or the Authorization Enforcement Proxy.

- **Authorization Enforcement Agent** generally provided by the authorization server vendor, is installed on the on the web application server. These agents generally conform to the web servers' native architecture. For example, there is a *module* for Apache®; a *filter* for Microsoft™ Internet Information Server® (IIS); an *extension* for iPlanet®, and so on. These will be referred to simply as Agents throughout this document. NOTE: the web or application server software itself is generally not part of the TOE and neither is part of the evaluation. Essentially, these Agents replace or augment the web server's native security mechanisms. The Agent runs in the same process as the web server itself and is invoked whenever the web server needs to determine access rights for a particular Uniform Resource Identifier (URI). The Web Server Agent forwards access requests and the principal identity information to the Authorization Server using the Access Control Decision API. The Policy Engine in the Authorization Server makes the access control decision and passes the answers back to the Agent. The Agent then enforces the decision by granting or denying the user access to the resource.

- **Authorization Enforcement Proxy** resides in the network topology between the principals and the resources being requested. In this case, the request from the principal (e.g. the HTTP request) will be examined to identify the resources and the operations being requested. The proxy will authenticate the principal, and interface to the Authorization Server (using the Access Control Decision API) to obtain a grant or deny decision. Based on that decision, the proxy will then either permit the request by transferring to the HTTP to the appropriate location, or will deny access to the user (displaying a static access denied page, or redirecting to a registration site, etc).

Attribute Authority*:* Authorization Server software products may provide an API that enables designated custom applications or databases to obtain user entitlements from the PADS. This API allows the Authorization Server software to function as an "Attribute Authority" to support various IT resources that need user attributes to make their own access control decisions. When the API receives the request for a user attribute, it must first validate the identity of the requesting software entity and ensure it is authorized to use the API. The API would have an interface to the PADS from which it would obtain the user entitlement. The API would then return the attribute values requested to the application or database making the request.

Authorization Server*:* Some Authorization Server products include Identification and Authentication (I&A) of principals. When I&A functionality is included, the Authorization Server product generally supports multiple mechanisms. The most common are user name/passwords and X.509 PKI certificates, but others include Windows Domain Authentication, Microsoft Passport, Liberty Alliance, RSA's SecureID, s/key, etc. The component that performs these services for the TOE is called the Authentication Server.

The Authentication Server may rely solely on information in the Privilege Attribute Data Store, for example in the case of password based authentication, when the password or a hash thereof may be validated by comparing the value stored in the PADS.

6. Documentation

U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0, Dated June 22, 2005.

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Developer Actions in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Section 12, Evaluation Results Summary, in the Evaluation Team's ETR, states:

"The evaluation team determined that the PPASBRE has successfully passed a Common Criteria APE evaluation."

8. Validation Comments/Recommendations

The validation team had no recommendations concerning the U. S. Government Protection Profile Authorization Server for Basic Robustness Environments, Version 1.0.

Comments

NOTE: While several components are mandatory, the ST author has an option to include some components or not. Based upon the components selected to be included in the TOE by the ST author, certain security functional requirements (SFRs) may not be included in the ST and certain SFRS must be operated upon in a specific manner. The PP author uses Application Notes to provide this clarification.

NOTE: SFRs can always be added. An example is the PP only includes single authorization mechanisms if a product contains multiple authorization mechanisms then the ST author should add the SFR FAI.UAU.5.

NOTE: The FIA_ATD.1(3) includes a selection of "none" which the PP author, evaluation team, and validator believes to be appropriate only because this is an iteration of the SFR, and this iteration may not apply to all products.

9. Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CIM	Consistency Instruction Manual for Development of U.S. Government Protection Profiles for Use in Basic Robustness Environments
CM	Configuration Management
COTS	Commercial off the shelf
CSP	Critical Security Parameters
DAC	Discretionary Access Control
DID	Defense in Depth
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IATF	Information Assurance Technical Framework
IT	Information Technology
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
PPRB	Protection Profile Review Board
QA	Quality Assurance
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTAP/CCEVS	Trusted Technology Assessment Program / Common Criteria Evaluation and Validation Scheme

10. Bibliography

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, CCIMB-2004-03-001, Version 2.4, dated March 2004

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, CCIMB-2004-01-002, Version 2.2, dated January 2004.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: CCIMB-2004-03-003, Version 2.2, dated March 2004.

[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.

[CEM_ASE/APE] Common Evaluation Methodology for Information Technology Security, ASE/APE Trial Use version 2.4, Revision 256, dated March 2004.

[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.

[PPRB_CG_Basic] Protection Profile Review Board, Protection Profile Consistency Guidance for Basic Robustness, Version 2.0, dated 1 March 2004