National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

webMethods Fabric 6.5

Report Number: CCEVS-VR-05-0136
Dated: 2005-12-23
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

Table of Contents

1. Executive Summary

This document is intended to assist the end-user of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST) which is where specific security claims are made, and this Validation Report (VR) which describes how those security claims were evaluated.

The evaluation of the webMethods Fabric 6.5 application integration software product was performed by CygnaCom Solutions, Inc. (an Entrust Company) in the United States and was completed on 5 December, 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2 (EAL2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.2.

CygnaCom Solutions, Inc. is an approved NIAP Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of webMethods Fabric 6.5 by any agency of the US Government and no warranty of the product is either expressed or implied.

1.1 webMethods Fabric 6.5 Functionality

webMethods Fabric is a client/server application that provides access control of services implemented on the webMethods Integration Server. The product facilitates the secure exchange of data and logic among resources and supports the development and management of complex business processes through browser or web enabled interfaces.

webMethods Fabric performs the following security functions, which are described in Section 3 of this report:

- Access Control Policy
- Identification & Authentication
- Security Management
- Self Protection
- Security Audit

1.2 Evaluation Details

Table 1-1 provides the required evaluation identification details.

Table 1-1. Evaluation Details

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	webMethods Fabric 6.5
EAL	EAL2
Protection Profile	None
Security Target	webMethods Fabric 6.5 Security Target, Version 1.0, 12 December, 2005
Developer	webMethods, Inc. 3877 Fairfax Ridge Road Fairfax, VA 20030
Evaluators	Swapna Katikaneni CygnaCom Solutions, Inc. 7925 Jones Branch Drive, McLean, VA 22102-3321
Validator	Ralph Broom Mitretek Systems, Inc., 3150 Fairview Park Drive South Falls Church, VA 22042
Dates of Evaluation	3 March, 2005 to 5 December, 2005
Conformance Result	Part 2 extended, Part 3 conformant, and EAL2 conformant
Common Criteria (CC) Version	CC, version 2.2, January 2004
Common Evaluation Methodology (CEM) Version	CEM version 2.2, January 2004
Evaluation Technical Report	webMethods Fabric 6.5 Evaluation Technical Report: - Volume 1, Evaluation Technical Report for a Target of Evaluation, ETR v1.0 dated 28 November, 2005. - Volume 2, Evaluation Technical Report for a Target of Evaluation, ETR v1.0 dated 18 November, 2005.
Key words	Business Software Integration

1.3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that **none** of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below were applicable to this evaluation. The Validator reviewed the relevant international interpretations and determined that the Evaluation Team correctly performed this analysis. The following international interpretations were reviewed by the Validator: 86, 137, 146, 175, 180, 192, 220, 227, 228, 232, 243 and 254.

2. Identification of the TOE

2.1 Software

webMethods Fabric 6.5 is a client/server application that provides access control of services implemented on the webMethods Integration Server (IS). The TOE facilitates the secure exchange of data and logic among resources and supports the development and management of complex business processes through web-enabled or browser interfaces.

The TOE consists of two primary components:

- Integration Server (IS) – Enables access control over the integration logic through the integrated applications
- Broker – A high-speed message router which enables access control over asynchronous messaging

The TOE also contains several secondary components:

- Host Adapters – Zero or more special modules that link back-end resources with the Integration Server. In this relationship the IS plays the role of the client to the external resource. The TOE includes two adapters; Java Database Connectivity (JDBC) for Oracle, Microsoft SQL Server, IBM DB2, and other databases, and Java Message Service (JMS) to permit high-speed asynchronous message delivery. Note that adapters rely on 3rd party drivers which are not part of the TOE.
- Developer – A graphical Integrated Development Environment (IDE) tool used by administrators to build, edit and test integration logic.

The following components are supplied with the TOE, but are not part of the TOE and were not evaluated:

- Entrust Authority Security Toolkit for Java 7.0 – provides cryptographic services for externals users and the Developer component connecting to the IS.
- Spyrus SSL Toolkit – provides cryptographic services (encryption) for connections between TOE components where one of them is a Broker or for the remote connection of an authorized administrator to the TOE.

The TOE consumer will need to provide the following:

- Appropriate hardware to run the operating system.
- A supported operating system to host the TOE.
- Appropriate network environment.
- Trained administrators; and
- Physical security of the TOE.

2.2 Documentation

The following documents were used to validate the evaluation:

- Security Target v1.0 for webMethods Fabric 6.5, dated 2005-12-12.
- Evaluation Technical Report Volume 1 for webMethods Fabric 6.5, ETR version 1.0 dated 2005-11-28.
- Evaluation Technical Report Volume 2 for webMethods Fabric 6.5, ETR version 1.0 dated 2005-11-18.
- webMethods Fabric 6.5 Proprietary Development Specification v0.6, dated 2005-11-17.
- webMethods Integration Server Administrator's Guide, Version 6.5, Document ID: webM-IS-AG-20040116webM-IS-AG-65-20050429.
- webMethods Broker Administrator's Guide, Version 6.5, Document ID: BR-AG-65-20050615.
- webMethods Fabric 6.5 Security Best Practices, December 2005.
- webMethods Fabric Version 6.5 Configuration Management v0.5 dated 2005-11-14.
- webMethods Fabric Version 6.5 CC Guidance Documentation v0.3 dated 2005-11-17.
- webMethods Fabric Version 6.5 Delivery Procedures v0.3 dated 2005-10-18.
- webMethods Fabric Version 6.5 Strength of Function Analysis v0.3 dated 2005-10-18.
- webMethods Fabric Version 6.5 Test Coverage Analysis v0.4 dated 2005-11-02.
- webMethods Fabric Version 6.5 Vulnerability Analysis v0.3 dated 2005-10-18.
- webMethods Fabric JDBC Adapter User's Guide, Document ID: ADAPTER-JDBC-UG-603-20040511
- webMethods Fabric JMS Adapter Installation Guide, Document ID: ADAPTER-JMS-IG-61-20040213
- webMethods Fabric JMS Adapter User's Guide, Document ID: ADAPTER-JMS-UG-61-20040213

3. Security Policy

webMethods Fabric 6.5 performs the following security functions:

- Access Control Policy
- Identification & Authentication
- Security Management
- Self Protection
- Security Audit

3.1 Access Control Policy

webMethods Fabric 6.5 enforces a discretionary information flow control policy to control access to services and documents based on users and groups. Documents are associated with document types, which define the structure of a particular type of document and how it is to be routed between Broker clients and resources. Services are logical methods that operate on documents, and are executed on the Integration Server.

Access control mechanisms are implemented on TCP ports and on resources. Port restrictions can be by either source or destination. Access to resources is controlled at the group level. The ability to define access control restrictions is limited to authorized administrators.

3.2 Identification and Authentication

webMethods Fabric 6.5 allows only users who have been successfully identified and authenticated (authorized administrators) to access security-relevant functionality, including viewing audit records. For password-based access, the TOE maintains a list of user accounts and data about these accounts: name, credential data, and a list of privileges. The TOE also supports certificate-based authentication of external users via the IT environment. (Certificate-based authentication was not evaluated.) The TOE identifies and authenticates users (based on user name and password) before allowing them to assume the administrative role defined by their privileges. No user may perform any administrative functions unless the identification and authentication are successful.

3.3 Security Management

webMethods Fabric 6.5 supports one administrative role to perform security management. An administrator can access the TOE remotely and monitor or manage the interaction between external users. An administrator can also access the Broker Server to manage the interaction between TOE components, or access through the Developer interface to configure or develop services or workflows.

3.4 Self Protection

webMethods Fabric 6.5 ensures that all information must flow through policy enforcement mechanisms and protects its programs and data from unauthorized access through its own interfaces.

3.5 Security Audit

The TOE generates audit information for security-relevant events and enables authorized administrators to view the audit records.

The TOE generates audit records for the following events:

- Reading of information from the audit records
- Unsuccessful attempts to read information from the audit records
- Modification of the audit configuration that occur while the audit collection functions are operating
- All requests to perform an operation on a package, folder, service, flow service, specification, schema, document type, or trigger
- Rejection by the TSF of any tested secret
- Modification of the behaviour of the functions in the TSF
- Modification of the values of security attributes
- Modification of the default setting of permissive or restrictive rules
- Modification of the initial values of security attributes
- All modification of the values of TSF data
- Use of the management functions
- Modification of the group of users that are part of a role
- start-up and shutdown of the audit function

Each audit record includes the date and time as obtained from the IT environment (OS), user identity (when applicable), type of event, and its outcome (success or failure). The audit records can be viewed by authorized administrators.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the TOE is expected to operate.

4.1 Usage Assumptions

The assumptions listed below are not addressed by any IT requirements but instead rely on the procedural or administrative measures applied to the operating environment. Users must consider these assumptions and whether they are valid for the intended use of the product.

A.Admin	The administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
A.Manage	It is assumed that one or more administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
A.NoUntrusted	It is assumed that there will be no untrusted software on the webMethods Integration Server and Broker.
A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
A.Users	It is assumed that users will protect their authentication data.
A.IT	The TOE relies upon the IT environment to support protected communications, provide audit file protection, support partial domain separation, support non-bypassability, provide reliable time-stamps, and to perform user authentication when configured to do so.

4.2 Environmental Threats

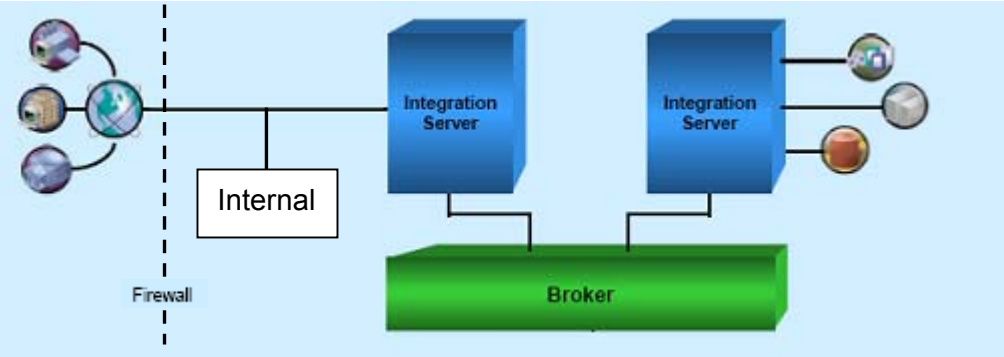
T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform.
T.Access	An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.
T.Bypass	An unauthorised user may attempt to bypass the information flow control policy.
T.Intercept	An unauthorized person on an internal network that connects TOE components may intercept communications between the TOE components and attempt to access and/or modify the data being transmitted.
T.Mismanage	Authorized Administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.

T.Tamper	An attacker may attempt to modify TSF programs and data.
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.
T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

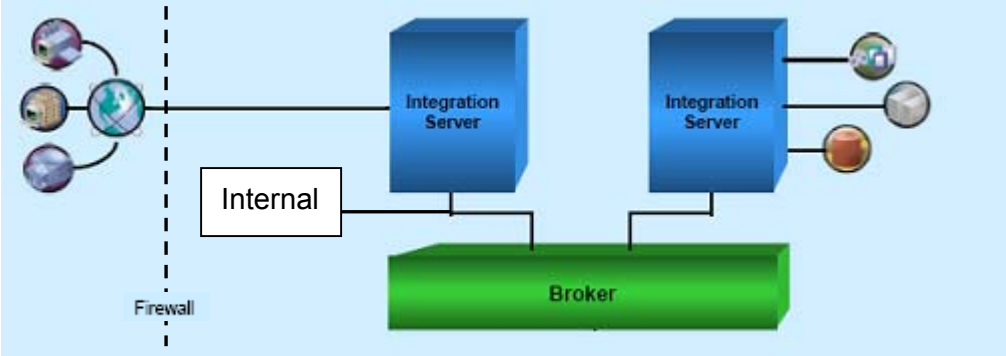
5. Evaluated Configuration

The three evaluated configurations consist of three machines running the Java Virtual Machine (JVM) version 1.4.2. Two machines ran the Integration Server (IS), and the third ran the Broker.

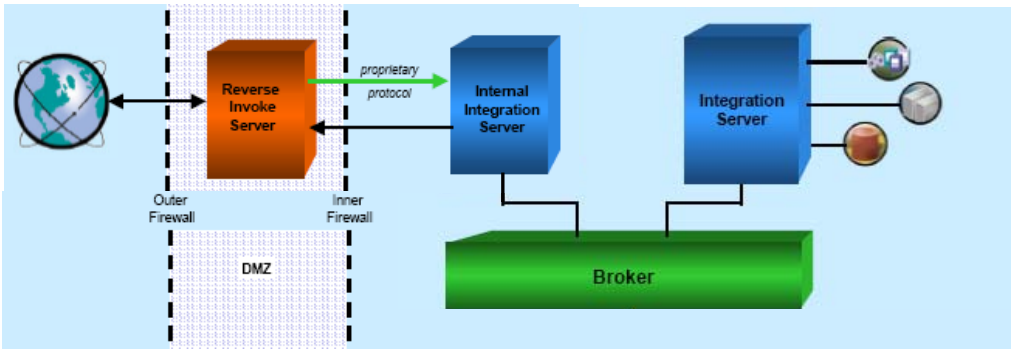
The first configuration involved users accessing a single IS via protected network ports.



The second configuration has the IS and Broker servers procedurally segregated (e.g., through encryption or trust) from the TOE. In this diagram the Broker and both Integration Servers are externally visible. For this configuration, the IT environment has to protect network connections.



The third configuration involves the IS and Broker servers running procedurally segregated users from behind a VPN. The Reverse Invoke server shown in this diagram is not part of the TOE. In this configuration, the TOE is accessed through a firewall and may not be directly connected to by external users.



5.1 Architectural Information

The TOE consists of three subsystems: the Integration Server, the Developer and the Broker.

The Integration Server contains the following interfaces:

- Graphical User Interface to the IS Administrator Interface
- Broker Administrative Interface
- External User Interface

The external interfaces on the Integration Server provide the following security functions:

- Access Control
- Identification and Authentication
- Security Management Functions
- Security Audit

The Developer interfaces with the Integration Server and provides the following functions:

- Adapter Services – Services that invoke specific processes on a back-end resource (for example, query a customer database, post a journal entry to a general ledger application, or delete an item from an inventory system).
- Adapter notifications — Alerts that are issued by back-end systems and which initiate an action on the integration platform.
- Adding Groups to ACL — The Developer is responsible for assigning ACL to the appropriate resource or resource folder.

All Developer functions are subject to the security functions of the Integration Server

The Broker has a single internal interface to the Integration Server and does not itself support any TOE security functionality. Access to the Broker is subject to the security functions of the Integration Server.

6. Evaluation and Validation Process and Conclusions

This section describes the evaluation process used by the team and the activities the Validator performed to gain confidence in the evaluation team's analysis.

The evaluation team conducted a review of the Integration Server, Developer and Broker components of the product based on functional requirements as specified in the Security Target and assurance requirements as required for EAL2.

The EAL2 assurance requirements include the following:

Table 6-1. EAL2 Components

EAL2 Component	EAL2 Component Title
ASE	Evaluation of Security Target
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

6.1 Evaluation of the Security Target (ASE)

The evaluation team applied each EAL2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies. The team also confirmed that the ST contains a statement of security requirements claimed to be met by the webMethods Fabric 6.5 product that are consistent with the Common Criteria, and product security function descriptions that support those requirements.

The Validator reviewed the Evaluation team's work units and compared them with the Security Target to determine that the work units were performed correctly.

6.2 Evaluation of the Configuration Management Capabilities (ACM)

Configuration Management (CM) systems are put in place to provide a method of tracking changes to the portions of the TOE that they control. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; that the configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. **The consumer must request the evaluated version of the product.**

The evaluation team analyzed the CM process and determined that TOE components and documentation have unique references and that a system is in place to track release configurations of the TOE and changes to its components.

The Validator reviewed the Evaluations team's work units and evidence to determine that the work units were performed correctly.

6.3 Evaluation of Delivery and Operations Documents (ADO)

The evaluation team analyzed the documentation of the procedures used to ensure that the TOE is delivered, installed, generated and started in the same way that the developer intended it to be and that it was delivered without modification. **The consumer must obtain the appropriate evaluation configuration documentation from the webMethods Advantage website (http://advantage.webMethods.com).**

The Validator reviewed the Evaluations team's work units, evidence and TOE documentation to determine that the work units were performed correctly.

6.4 Evaluation of the Development (ADV)

The evaluation team inspected the design documentation to determine that the TOE Security Functions (TSF) could be understood, were consistent and that they supported the claims in the ST. The design documentation consists of a functional specification describing the TOE in terms of internal subsystems and a high-level design which describes how those subsystems work together.

The Validator reviewed the Evaluations team's work units, the TOE functional specification and user and administrator guidance to determine that the work units were performed correctly.

6.5 Evaluation of the Guidance Documents (AGD)

The evaluation team analyzed the documentation that describes how to operate the TOE in a secure manner and compared it with the actual operation of the TOE. The TOE Broker component includes both a Graphical User Interface (GUI) and a command-line interface; only the GUI was evaluated.

The Validator reviewed the Evaluations team's work units, test results and user and administrator guidance to determine that the work units were performed correctly.

6.6 Evaluation of the Test Documentation and Testing Activity (ATE)

The evaluation team examined the developer tests to ensure that those tests would confirm that the TOE behaves as specified in the design documentation and in accordance with the TSF requirements as specified in the ST. In addition, the evaluation team independently performed a subset of the developer tests and compared them to the developer test results.

The Validator reviewed the Evaluations team's work units, test results and developer test results to determine that the work units were performed correctly.

6.7 Vulnerability Assessment Activity (AVA)

The evaluation team examined the TOE for flaws or weaknesses in its intended environment and conducted its own penetration testing. The team reviewed the developer's claims for the strength of specific security functions, performed searches for obvious vulnerabilities and conducted a sample penetration test.

The Validator reviewed the Evaluations team's work units, test results and penetration test to determine that the work units were performed correctly.

6.8 Summary of the Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the majority of the vendor test suite also demonstrates the veracity of the claims in the ST.

7. IT Product Testing

Testing was conducted from 20 October, 2005 to 24 October, 2005 at the webMethods facility in Fairfax, VA. The testing was conducted by Swapna Katikaneni, representing the CCTL CygnaCom. Functional and vulnerability testing was conducted, including a partial execution (~80%) of the developer test suite with a focus on authentication and access control functionality. Delivery and installation procedures were also examined. The Broker and its functions were excluded from the list of TOE Security Functions and testing.

The test configuration was as described in section 5. Evaluated Configuration, with the JVM running on Windows XP SP2. The approach used was functional test-case design.

8. Validator Comments/Recommendations

This is a software-only TOE. The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices.

The Validator has the following observations:

- In order to meet requirements for auditing the end-user must install the Integration Server WmCCudit package as described and follow the procedures outlined under Auditing in the Evaluated Configuration in Appendix C of the webMethods Fabric 6.5 Security Best Practices document.

- The developer tests fully or partially covered all TOE security functional requirements and the evaluator executed approximately 80% of the developer tests as well as additional independent tests. All TOE security functions and their interfaces were tested.

- Configuration of this product is moderately complex; however the administrative guidance is helpful in supplying explanations of configurable options, useful default values and warnings of possible unsafe values or configurations.

- The TOE uses cryptography (SSL) in the IT Environment to protect communications between TOE components. Cryptography was not part of the TOE evaluation, so intra-TOE communications should be protected (e.g., isolated from untrusted networks), or the end-user (or product installer) should consider the risks of using a non-evaluated cryptographic implementation to protect the communication path.

- Although the installer was not part of the TOE evaluation, testing did determine that it correctly installed the TOE.

The Validator agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 2.

The Validator therefore concludes that the evaluation and the Pass results for the TOE identified below is complete and correct:

webMethods Fabric 6.5

9. Security Target

The Security Target (ST) reference for this product is "webMethods Fabric 6.5, EAL2 Common Criteria Evaluation, Security Target V1.0, 12 December 2005". The ST describes what the TOE does, defines the functional claims that the developer is making for the TOE and which standards / specifications the TOE is claimed to conform with.

The conformance claims for this product are:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, January 2004, CCIMB-2004-01-002, at Evaluation Assurance Level (EAL) 2.

10. List of Acronyms

Acronym	Definition
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
EAL2	Evaluation Assurance Level 2
ETR	Evaluation Technical Report
GUI	Graphical User Interface
NIAP	National Information Assurance Partnership
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions

11. Bibliography

In addition to the documents specified in section 2.2 Documentation, the following documents were used in compiling this Validation Report:

- Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:
  - Part 1: Introduction and General Model
  - Part 2: Security Functional Requirements

  - Part 2: Annexes
  - Part 3: Security Assurance Requirements
- Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004: