Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/77

09 Sept 2011

Version 1.0

Amendment Record

Version	Date	Description
0.1	22/08/2011	Internal release.
0.2	26/08/2011	Extended review.
1.0	09/09/2011	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the IBM Tivoli Storage Manager 6.2.1 Extended Edition which is a data backup, archive and restoration software solution.

2 This report describes the findings of the IT security evaluation of IBM's Tivoli Storage Manager 6.2.1 Extended Edition, to the Common Criteria (CC) evaluation assurance level EAL 3 + ALC_FLR.1. The report concludes that the product has met the target assurance level of EAL 3 + ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by AISEF stratsec and was completed on 1st August 2011.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users and administrators:

a) Use the product in its evaluated configuration;

b) The administrator should check the operational requirements and compatibility with deployed infrastructure;

c) The administrators must ensure that the TOE is physically secured to ensure appropriate protection of residual information;

d) The administrator should have a thorough understanding of how the environment must be set up.

e) The administrator should be familiar with system requirements, integration into existing architectures and the application of certificate authorities; and

f) Upon successful installation of the TOE, the installation of the DB2 database should be assessed to ensure that it is up to date and securely configured.

4 This report includes information about the underlying security policies and architecture of the TOE and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target (Ref [1]) and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE, Tivoli Storage Manager 6.2.1 Extended Edition, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 3 + ALC_FLR.1; and

b) Provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 0 .

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Tivoli Storage Manager 6.2.1 Extended Edition
Software Version	Tivoli Storage Manager 6.2.1 Extended Edition
Security Target	Tivoli Storage manager 6.2.1 Security Target version 2.8, release 9 August 2011
Evaluation Level	EAL 3 + ALC_FLR.1
Evaluation Technical Report	EFS-T025 ETR 1.0, release 1 August 2011
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. CCMB-2009-07-001, CCMB-2009-07-002, & CCMB-2009-07-003
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.
Conformance	Common Criteria Part 2 Extended Common Criteria Part 3 Augmented
Sponsor & Developer	IBM Corporation 1 New Orchard Road Armonk, New York 10504-1722 United States 914-499-1900
Evaluation Facility	AISEF stratsec Suite 1, 50 Geils Court, Deakin, ACT 2600

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Tivoli Storage Manager 6.2.1 Extended Edition developed by IBM. Its primary role is to act as a data backup, archive and restoration software solution.

12 The TOE supports backup of Network Attached Storage (NAS) file server directly to the IBM Tivoli Storage Manager (TSM) Server. (See Figure 1 - Diagram of the TOE). The TSM also provides for the retrieval and restoration of the data from the Server Node to the Client Node or NAS file server as well as providing functions for the management of the TOE and its data.

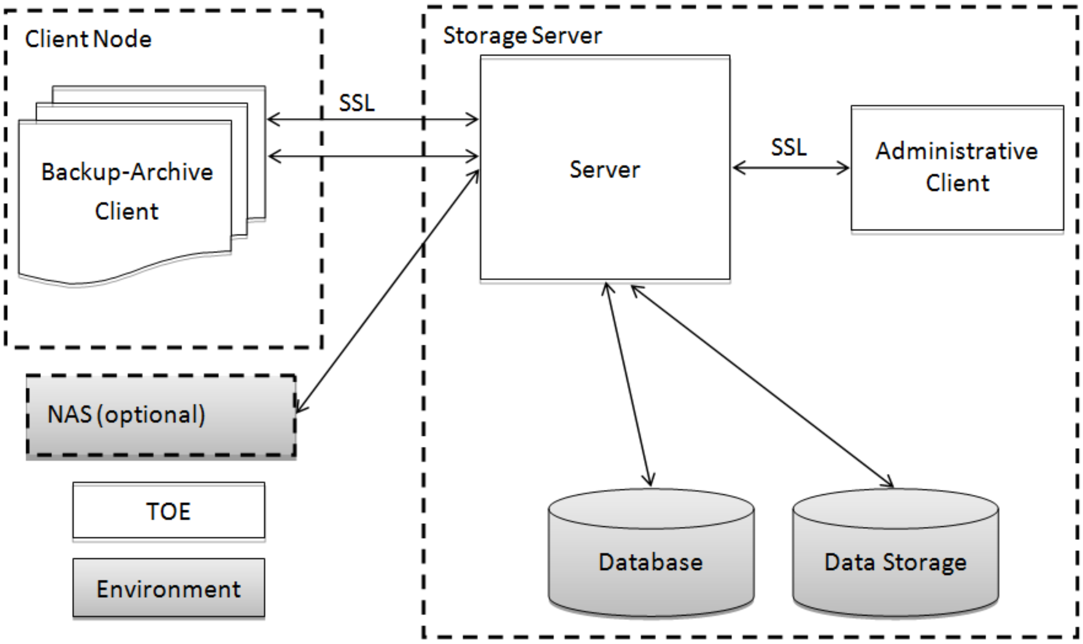

Figure 1 - Diagram of the TOE

13 The TOE provides password quality enforcement for authentication passwords including password expiration. It also supports password generation for both authentication and data encryption passwords.

14 **Identification & Authentication**

15 The server makes use of an IBM DB2 database to store user and administrator account details, separate from the operating system's user account database. The TOE defines two account types: client node and administrators. The server requires all accounts except for the predefined SERVER_CONSOLE administrator account to be identified and

authenticated before providing access. The SERVER_CONSOLE administrator account is only available through direct access to the server's command line interface (known as the TSM Server console or simply the server console). As no identification or authentication is required for access to the SERVER_CONSOLE account, the TSM Server is required to be protected by appropriate physical security measures. Direct access to the TSM Server is possible only through the SERVER_CONSOLE account. The quality of passwords used can be enforced through configuration options controlled by the TOE. Automatic password generation is supported on Backup-Archive (B/A) Clients. User and administration accounts can only be created at the server, either by using the server console directly or by a *system* level administrator using the administration console.

16 The TOE uses TLSv1 communication between the TSM B/A Client and the TSM Server and between the TSM Administration Client and TSM Server, requiring the server to authenticate to the client using X.509 certificates. Mutual authentication is achieved by combining the TLS certificate authentication with the password-based identification and authentication required by the server.

17 Access Control

18 The backup and archive data saved by a client node account to a server are protected by an editable list of rules. By default client node accounts can only access their own data, but a client node account can modify its list of rules to grant other client node accounts access to one or more backup and archive objects owned by the client node account. It can also remove rules from the list, thereby denying previously granted access. Each rule includes the name of the client node allowed access, the name of the client node account allowed access and the name of the object that they are allowed to access and whether the object name refers to a backup or archive object.

19 Secure Communications

20 The TOE uses TLSv1 communications between distributed subsystems of the TOE to protect the data (including TSF data) transferred between these components. This functionality is provided through the use of IBM's IBM Global Security Kit (GSKit) module. GSKit includes the IBM Crypto for C (ICC) cryptographic module, which is FIPS 140-2 approved. GSKit ensures that only secure values are accepted for the attributes governing cryptographic key management and cryptographic operations.

21 Security Management

22 The management of security critical parameters of the TOE is performed by the administrators of the TOE. The TOE must be used and administered by operating system administrators only. Command line interfaces are provided to manage many of the security features and parameters of the TOE. The TOE also contains configuration files whose access is limited to operating system administrators. The TOE supports privilege classes and client access authorities for administrative accounts, allowing administrative power to be restricted for specific roles.

2.3 Security Policy

23 The Security Policy is a set of rules that defines how the information within the TOE is managed and protected defined in the Security Target (Ref [1]). A summary of the Security Policy is provided below:

a) Password security policy. The TOE supports setting the passwords both globally and per account.

2.4 TOE Architecture

24 The TOE consists of the following major architectural components:

a) The B/A Client Command Line Interface (CLI);

b) The B/A Client configuration file;

c) The B/A Client's password data;

d) The B/A Client's error log file;

e) The B/A Client Scheduler Agent's error log file;

f) The keystore files for the B/A Client and storage server;

g) The server program which includes the server console CLI;

h) The Administrative Client CLI which provides a command line interface to manage the server;

i) The IBM Global Security Kit (GSKit 7d for server and GSKit 8.0.13 for client) library package providing SSLv3/TLSv1 support for the Client Node, Administrative Client and server and includes the ICC version 1.4.5 – a FIPS approved cryptographic library containing the following algorithms;

   i) AES 128 bit and 256 bit;
   ii) TDES 168 bit;
   iii) SHA-1 digest algorithm;
   iv) Random number generator; and
   v) Server configuration files.

25 The TOE runs on a general purpose multi-user operating systems. In the evaluated configuration, the only individuals allowed to use the TOE are the operating system administrators. All executable files and data files are protected from non-OS administrative access by the use of access control mechanisms of the operating systems in the environment.

26 The client/server design provides a natural boundary for scoping administrative tasks. Administrators logged into the B/A Client can only manage the B/A Client and the backup/archive data on the server associated with that Client Node. They cannot perform server specific management functions. Administrators logged in via the Administrative Client or Server Console can only perform server related administrative tasks such as user account management. The Administrative Client CLI and Server Console CLI provide nearly identical command line interfaces. The only difference is that the Server Console does not support the

database SELECT command used to perform SQL-like database queries in the Administrative Client CLI. They cannot directly manage a B/A Client.

27 In order to support a distributed TOE, the architecture provides secure communications using SSLv3 and TLSv1 for inter-TOE communication. This not only provides for mutual authentication between the client and server portions of the product, but it provides for data integrity and confidentiality. The server defines the set of acceptable cipher suites to be used during secure communications, not the Client Nodes. The B/A Client and Administrative Client have keystores which contain the server's public key (certificate). The server's keystore contains both its private and public key. The certificates are established when the parts of the TOE are installed. All keystores are protected by the operating system's access control mechanism(s) from unauthorised access.

28 The storage server also controls the creation and maintenance of accounts and the password policies used by all accounts.

29 The components that require cryptographic support use the same library package, GSKit, to provide these services. The ICC portion of GSKit has been FIPS 140-2 approved, thus, providing assurance of quality cryptographic functionality.

2.5 Clarification of Scope

30 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

31 The TOE provides the following evaluated security functionality:

a) Identification and authentication;

b) Access control;

c) Secure communications: IBM use Global Secure ToolKit (GSKit) which is a set of programmable interfaces that allow an application to be SSL enabled; and

d) Security management.

2.5.2 Non-evaluated Functionality and Services.

32 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 0) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

33 The functions and services that have not been included as part of the evaluation are provided below:

a) Data storage;

b) Database;

c) Client acceptor daemon;

d) Scheduler agent;

e) Logical volume snapshot agent; and

f) Journal engine service (Windows)

2.6 Usage

2.6.1 Evaluated Configuration

34 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref 0) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

35 The installation guides for Windows and AIX detail the methods to install the TOE to a default configuration on the supported Windows and AIX operating systems. The evaluated configuration is detailed in the ST (ref [1]) and the IBM Tivoli Storage Manager, Common Criteria Guide 6.2.1 (Ref [3]). The evaluated configuration is based on the default installation of the TOE with additional requirements summarised below:

a) The TOE is IBM Tivoli Storage Manager v6.2.1, both the basic and extended editions. The evaluated configuration includes both the server component and the backup-archive client (B/A Client) component.

b) The evaluated configuration (B/A Client and TSM Server) is supported on Microsoft Windows Server 2003 SP2 (32-bit or 64-bit), Microsoft Windows Server 2008 (32-bit or 64-bit) and IBM AIX 6.1(64-bit).

c) The TOE is configured as a single server with multiple client nodes (server to server communications is excluded from the evaluated configuration).

d) The server user account type is not supported in the evaluated configuration and should not be created. Only administrator and client node user accounts are supported

e) The evaluated configuration includes the server console (when invoked from a command line) which allows access to the SERVER_CONSOLE administrative account.

f) Communications between the server and client nodes (including the web client) must use SSL/TLS.

g) Password policy must be enforced with the following metrics:

i) Minimum length of a password: 8 characters

ii) Maximum lifetime of a password: 90 days

iii) Maximum number of consecutive failed logon attempts: 3 attempts

iv) Server must have password authentication configured ("set authentication on" in server options file).

h) The TSM Server must have node registration set to closed (i.e. only administrators can register nodes).

i) Client password access option must be set to prompt (except when using the web client).

j) The IBM DB2 v9.7 database supplied as part of the TSM Server is regarded as part of the environment.

k) The TSM data storage and any (optional) NDMP-compliant network attached storage (NAS) file server are regarded as part of the environment.

2.6.2 Hardware prerequisites:

36 The following are the recommended minimum hardware requirements for the TOE:

37 **Windows**:

a) Intel Pentium compatible processor or multiprocessor-based computer;

b) At least 3GB of free disk storage, at least a 2GB partition size in the C:\ drive, 200MB temporary directory space and 300MB in the instance directory. Significant additional disk space is required for database and log files; and

c) At least the following amounts of memory:

i) 64-bit Windows: 12GB (16GB if using deduplication). For multiple instances, each instance requires the memory listed for one server.

ii) 32-bit Windows: 8GB (deduplication is not supported). Running more than one server instance on a system is not supported.

iii) The packaging includes GSKit 7d for server and GSKit 8.0.13 for client. Only the TOE components for the operating systems mentioned in section.

38 **AIX**:

a) An appropriately configured 64-bit p4, p5 or p6 System p computer;

b) At least 5MB for the /var directory, 10MB for the /opt directory if you create mount points, 2GB for the /opt/tivoli/tsm directory if you create mount points, 360MB for the /tmp directory, 300MB for the /usr directory and at least 2GB in the home directory. Significant additional disk space is required for database and log files;

c) At least 12GB of memory. For multiple instances, each instance requires the memory listed for one server.

2.6.3 Software prerequisites:

39 The following are the minimum software requirements needed to install the TOE:

40 **Windows**:

41 One of the following operating systems is required. Some functionality is not available on 32-bit systems.

a) Microsoft Windows Server 2003: Standard, Enterprise, or Datacenter Edition, Service Pack 2 or later.

b) Microsoft Windows Server 2003: Standard, Enterprise or Datacenter x64 Edition (64-bit), Service Pack 2 or later.

c) Microsoft Windows Storage Server 2003.

d) Microsoft Windows Storage Server 2003 x64.

e) Microsoft Windows Server 2008: Standard, Enterprise, or Datacenter Edition.

f) Microsoft Windows Server 2008: Standard, Enterprise, or Datacenter x64 Edition (64-bit).

g) Microsoft Windows Server 2008 R2: Standard, Enterprise, or Datacenter Edition.

42 At least one of the following communication protocols (installed by default with the current Windows operating systems):

a) Named Pipes.

b) TCP/IP Version 4 or Version 6.

43 **AIX**

44 AIX 6.1 running in a 64-bit kernel environment with the following additional requirements:

a) AIX 6.1 TL 2.

b) Minimum C++ runtime level with the xlC.rte.9.0.0.8 and xlC.aix61.rtte.9.0.0.8 file sets. These file sets are included in the June 2008 fix pack package for IBM C++ Runtime Environment Components for AIX.

c) A configured communication method.

d) Asynchronous I/O must be enabled.

45 **Additional Software**

46 A web browser is required to log in and use the console. The web browser can be installed on the same or a separate system. The following browsers are supported:

a) Microsoft Internet Explorer 6.0 SP1;

b) Microsoft Internet Explorer 7.0;

c) Firefox 2.0 or later; and

d) Mozilla 1.7.8.

2.6.4 Delivery procedures

47 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

2.6.5 Determining the Evaluated Configuration

48 In the evaluated configuration, the IBM Tivoli Storage Manager is delivered electronically. Before placing an order, the customer must enrol online in IBM's Passport Advantage program. Terms of the agreement and whether or not the customer must place an order of a minimum size are dependent on the customer type (commercial, government, academic) and the products and services desired by the customer.

49 More information about the Passport Advantage program, including a tutorial, is available at the website:

50 http://www-142.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/passporthome

51 Customers enrol online using the following website:

52 http://www-142.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/howtoenroll. Once enrolled in Passport Advantage, the customer may download the evaluated TOE, including documentation.

2.6.6 Order tracking

53 After the customer places an order, a six-digit number identifying the order is emailed to the customer. Each order number is stored in a database along with all of the associated customer and order information. This information is used both to track the order and to manage access so that the customer can access only the products they have purchased.

2.6.7 Order download

54 After enrolment in Passport Advantage, the customer can download the TOE from the Passport Advantage customer website.

55 The customer must first get IBM's Download Director – a Java applet available for download on the Passport Advantage customer website. Once the Download Director is downloaded it is used by the customer to connect to the Tequila server instance on the fulfilment server. Tequila is a client/server application that facilitates file downloads and provides the 'ticket' and secure hash security features described below. Tequila includes a server and an API and code library on the client, but does not itself provide a client-side user interface. Download Director provides this user interface. Download Director communicates with the Tequila server when downloading the IBM Tivoli Storage Manager.

56 In order to ensure security of the TOE, IBM mails a "ticket" to the customer that includes the IP address of the user downloading the TOE and is designed to expire after 5 hours. The Download Director uses the "ticket" when connecting to the Tequila instance on the fulfilment server and then each data segment downloaded by the Download Director is signed with a 20-byte SHA-1 secure hash. If a data segment is found to be

incorrect based on the hash, it is discarded and another copy of that segment is requested.

57 If the download fails for some other reason (such as a lost connection), Download Director automatically attempts to resume downloading the file or files. Download Director checks the secure hash upon resuming the download operation. If a problem occurs during the download process that Download Director cannot rectify (for example, the downloaded item appears to be the wrong product), the customer can contact IBM via phone to rectify the problem. The phone number is provided once the customer has enrolled in Passport Advantage.

58 For more information about Tequila, refer to the Tequila Functional Specification document.

59 The download obtains the following files which are compressed versions of the installation software for the identified product components. (The Windows versions are self-extracting zip files, while the AIX files are zipped tar archive files.

- CZG6SML.bin – IBM Tivoli Storage Manager V6.2.1 AIX Server Multilingual
- CZGL7ML.bin – IBM Tivoli Storage Manager V6.2.1 AIX Clients Multilingual
- CZG6ZML.exe – IBM Tivoli Storage Manager V6.2.1 Windows X64 Server Multilingual
- CZG70ML.exe – IBM Tivoli Storage Manager V6.2.1 Windows X32 Server Multilingual
- CZGM2ML.exe – IBM Tivoli Storage Manager V6.2.1 Windows Clients Multilingual

60 Other non-TOE files are downloaded and can be ignored (e.g., TSM for non-evaluated platforms, the Administration Centre and Reporting tools).

2.6.8 Order Security

61 The Electronic Release Lab makes the TOE available for download. The TOE is an eSD (Electronic Software Distribution) image based on the finalized release version of the software. When the Electronic Release Lab receives the eSD image, Electronic Release Lab personnel run a checksum program on the image and verify the results of the checksum by emailing the individual who provided the image.

62 The customer downloads the TOE using a Java applet called Download Director. Each segment of the download is signed with a 20-byte SHA-1 secure hash. Once each segment is downloaded, Download Director checks the hash for integrity. If the hash is invalid, the program discards the invalid segment and requests the segment again.

2.6.9 Physical security of download servers

63 The servers used in the download process reside in facilities where physical access is controlled according to IBM security policy. These

controlled access areas, referred to in the ITCS 204 document as CA areas, are locked at all times (even when in use). An individual designated as the “area owner” is assigned to manage each controlled access area. Only individuals authorized by the area owner may physically access the controlled access area. Only persons with a legitimate business need to physically access the area are granted such access.

64 For more information regarding the protection of IBM servers refer to IBM Corporate Standard ITCS 314 (“Business Unit Production system”) and IBM Corporate Standard ITCS 204: Security Standards for Essential Network and Computing Services.

2.6.10 Software security of download servers

65 The servers used in the process of downloading the TOE have mandatory access control and other software security measures placed on them according to IBM security policy. Identification and authentication is required in order to access server resources. If an individual who has been granted electronic access to a system leaves IBM, the user’s access to the system is revoked.

66 In order to maintain the integrity and security of each server, IBM security policy requires that identified software vulnerabilities be fixed or otherwise prevented from being exploitable over the Internet. Because some software vulnerabilities may be of critical importance, IBM security policy requires that “emergency fixes” be applied according to a timeframe defined on a case-by-case basis.

67 Servers are formally scanned periodically for TCP/IP vulnerabilities.

68 Servers are required to be “locked down” by disabling or changing operating system, device, or application settings that might render the server vulnerable to attack. IBM security policy documentation specifies the default settings that must be disabled or changed.

69 For more information regarding the protection of IBM servers refer to IBM Corporate Standard ITCS 314 (“Business Unit Production system”) and IBM Corporate Standard ITCS 204: Security Standards for Essential Network and Computing Services. For information regarding the protection of IBM networks, refer to IBM Corporate Standard ITCS 302: Security Standards for Inter-Enterprise Services.

2.6.11 Documentation

70 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. For a full list of the documentation available to customers of the TOE for download see: A.2 product documentation. This is available when the TOE is downloaded from the IBM support website.

2.6.12 Secure Usage

71 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met. For more information about this please see the ST (ref: [1])

72 Assumptions are made in the following areas:

a) Physical security;

b) Trusted administrators;

c) Secure runtime environment; and

d) Trusted software on the client node.

73 In addition, the following organisational security policies must be in place:

a) A policy stating the minimum security requirements for data encryption passwords exists and is enforced outside of the TOE.

Chapter 3 - Evaluation

3.1 Overview

74 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

75 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [3], [4] and [5]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [6]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [7], [8] and [9]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

3.3 Functional Testing

76 To gain confidence that the developer’s testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer’s testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

77 Penetration testing was conducted based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description as well as available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

78 The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

d) IT hardware/software or other equipment required for exploitation.

Chapter 4 - Certification

4.1 Overview

79 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen and recommendations made by the certifiers.

4.2 Certification Result

80 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of Tivoli Storage Manager 6.2.1 Extended Edition performed by the Australasian Information Security Evaluation Facility, AISEF stratsec.

81 AISEF stratsec has found that Tivoli Storage Manager 6.2.1 Extended Edition upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level EAL 3 + ALC_FLR.1.

82 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

83 EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and an architectural description of the design of the TOE, to understand the security behaviour.

84 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

85 EAL3 also provides assurance through the use of development environment controls, TOE configuration management and evidence of secure delivery procedures.

86 This EAL represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functionality and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.

4.4 Recommendations

87 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 0) and New Zealand Government users should consult the GCSB.

88 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref), the ACA also recommends that users and administrators:

a) The administrator should check the operational requirements and compatibility with deployed infrastructure;

b) The administrators must ensure that the TOE is physically secured to ensure appropriate protection of residual information; and

c) The administrator should have a thorough understanding of how the environment must be set up. The administrator should be familiar with requirements, integration into existing architectures and the application of certificate authorities.

d) Upon successful installation of the TOE, the installation of the DB2 database should be assessed to ensure that it is up to date and securely configured.

Annex A - References and Abbreviation

[1] Tivoli Storage manager 6.2.1 Security Target version 2.8, release 12 August 2011.

[2] Australian Government Information Security Manual (ISM), June 2011, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.

[7] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[8] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[9] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[12] Evaluation Technical Report for IBM Storage Manager v6.2.1 EFS-T025 ETR, 1 August 2011

A.1 User Documentation

[13] The TSM Publications include the TSM guidance documentation for each supported operating system. This includes the following :

- IBM Tivoli Storage Manager v6.2.1 Security Target Version 2.7
- IBM Tivoli Storage Manager v6.2.1: Using the Application Programming Interface
- IBM Tivoli Storage Manager for AIX v6.2.1: Administrator's Reference
- IBM Tivoli Storage Manager for Windows v6.2.1: Administrator's Reference
- IBM Tivoli Storage Manager for UNIX and Linux v6.2.1: Backup-Archive Clients Installation and User's Guide
- IBM Tivoli Storage Manager for Windows v6.2.1: Backup-Archive Clients Installation and User's Guide
- IBM Tivoli Storage Manager for AIX v6.2.1: Installation Guide
- IBM Tivoli Storage Manager for Windows v6.2.1: Installation Guide
- IBM Tivoli Storage Manager for AIX v6.2.1: Administrator's Guide
- IBM Tivoli Storage Manager for Windows v6.2.1: Administrator's Guide
- TSM 6.2.1 for Windows and AIX, Configuration Management Plan, Edition 5
- IBM Tivoli Storage Manager, Delivery Procedures, Revision 9
- IBM Tivoli Storage Manager v6.2.1: Common Criteria Guide
- IBM Tivoli Storage Manager v6.2.1: Security Architecture Document, Version 0.2
- IBM Tivoli Storage Manager v6.2.1: Life Cycle Support, Version 1.2 (31-March-2010)
- High Level Design & Functional Specification IBM Tivoli Storage Manager 6.2. Version 1.9
- IBM Tivoli Storage Manager v6.2.1 Impact Analysis Report Revision 0.4
- Notes on choosing a test platform.xlsx
- IBM Tivoli Storage Manager Common Criteria Test Plan v0.9
- ccsec009.pl (script for CCSEC009 test case)
- CCSEC010-manual

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
B/A	Backup/Archive client
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
eSD	Electronic Software Distribution
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
GCSB	Government Communications Security Bureau
GSKit	IBM Global Security Kit
ICC	IBM Crypto for C
ISM	Information Security Manual
NAS	Network Attached Storage
NDMP	Network Data Management Protocol
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
ST	Security Target
T-DES	Triple Data Encryption Standard
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
TSP	TOE Security Policy
TSM	Tivoli Storage Manager.
+	Augmented