Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/53

22 May 2009

Version 1.0

Amendment Record

Version	Date	Description
0.1	04/05/2009	Internal release.
0.2	15/05/2009	Extended review.
1.0	22/05/2009	Public release.

Executive Summary

1 IBM Tivoli Storage Manager v5.5.1 (TSM) is a software application that employs a client-server architecture to perform enterprise-wide data backup, archival, and restoration supporting multiple operating systems and multiple media storage types. The security target includes both client and server components. IBM Tivoli Storage Manager v5.5.1 is the target of evaluation (TOE).

2 This certification report describes the findings of the IT security evaluation of IBM Tivoli Storage Manager v5.5.1, to Common Criteria (CC) evaluation assurance level EAL3 augmented with ALC_FLR.1. The report concludes that the product has met the target assurance level of EAL3 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed in 10 Mar 2009.

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

a) The TOE be invoked as a service and managed via WMI when installed on a Windows 2003 Server host as the server console does not provide any authentication functionality. If the TOE is invoked from a command line (thus spawning an open console) suitable access controls must be applied over remote desktop services to prevent unauthorised access to the server console.

b) Appropriate physical access controls should also be applied to prevent unauthorised access to the server console. Passwords used to access the TOE are not case sensitive and are limited to: any letter a-z upper or lower case, any number 0-9, the underscore, a period, a hyphen, a plus sign, or an ampersand. Due to these limitations on the set of characters allowed for passwords, the evaluators recommend that TOE administrators enforce suitable minimum password lengths and expiry periods in the TOE configuration. Customers should also incorporate a TOE specific password policy into the relevant organisational security policies.

c) The evaluators noted that TOE administrative client software (dsmadmc.exe) automatically re-establishes a terminated idle connection when the user next attempts to execute any functions. The user is not prompted to re-enter a password if the client software is not terminated prior to executing the administrative commands. The evaluators recommend that the administration console be installed on an appropriately secured machine.

d) Finally, the evaluators observed during testing that data being archived or backed up from the BA Client components is encrypted using AES with 128-bit key lengths. If 256-bit encryption is

required, the data must be encrypted with a separate encryption utility prior to invoking a backup or archive operation.

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 at 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, IBM Tivoli Storage Manager v5.5.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL3 augmented with 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 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	IBM Tivoli Storage Manager v5.5.1 which includes the following components: • TSM Server • BA Client (Backup/Archive Client) GUI, Command line and Web Client • IBM Global Security Kit (GSKit7)
Software Version	IBM Tivoli Storage Manager v5.5.1
Security Target	IBM Tivoli Storage Manager v5.5.1
Evaluation Level	EAL3 augmented with ALC_FLR.1
Evaluation Technical Report	Evaluation Technical Report for IBM Tivoli Storage Manager v5.5.1, 20 March 2009

Criteria	CC Version 2.3, August 2005, with interpretations as of 18 July 2005.
Methodology	CEM-99/045 Version 2.3, August 2005 with interpretations as of 18 July 2005
Conformance	Part 2 extended Part 3 conformant, augmented with basic flaw remediation (ALC_FLR.1)
Sponsor	SAIC 7125 Columbia Gateway Drive Suite 300, M/S CM6-80 Columbia MD 21046
Developer	IBM 9000 S Rita Rd TUSCON AZ 85744-0002
Evaluation Facility	stratsec Suit 1/50 Geils Court Deakin, ACT

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 the IBM Tivoli Storage Manager v5.5.1 developed by IBM.

12 The TOE is a data backup, archive, and restoration software solution. It provides the ability to backup data from one or more computers, known as client nodes, to another computer known as the server node (see Figure 1 – TOE logical overview). The TOE also provides for the retrieval and restoration of data from the server node to the client node as well as providing functions for the management of the TOE and its data.

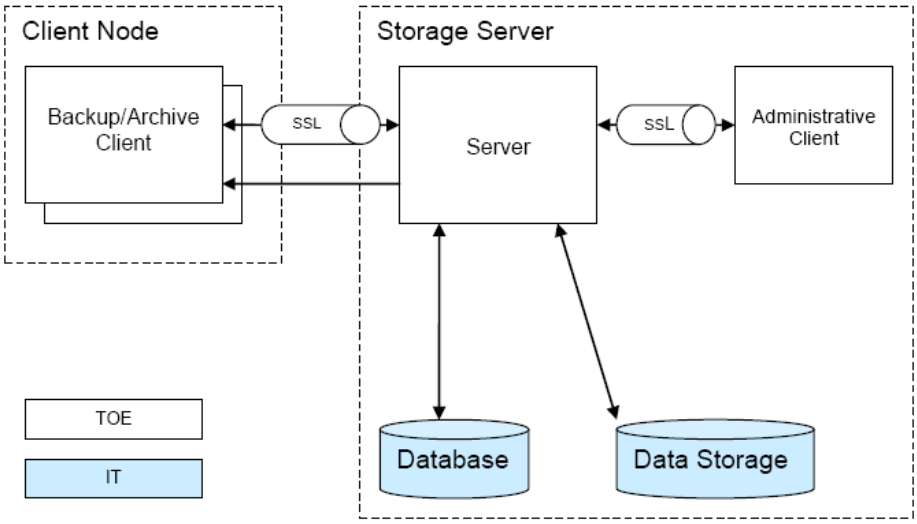

Figure 1 – TOE logical overview

13 The client node consists of the backup/archive client (a.k.a. B/A client). The server node is comprised of an administrative client CLI, database, data storage, and server (the server program being the hub of all activity). The B/A client software communicates directly with the server to backup and archive data to the storage server, restore data from the storage server, and manage data while it resides on the storage server. The B/A client also provide the command line interface for administrators of the client node to interact with the server. B/A clients communicate with the server over an SSL/TLS connection with a protocol that employs mutual authentication. Additionally, there is a unidirectional, unauthenticated communication path from the server to a B/A client that allows a server to request a predefined backup of the client node. This communications path is used for scheduled backups initiated by the server.

14 The administrative client CLI is a command line administrative interface that's used to manage the TOE and TOE data stored on the server node. It communicates to the server over an SSL/TLS connection with a protocol that employs mutual authentication.

15 Further details on the TOE and its operating environment are provided in the Security Target (Ref [1]).

2.3 Security Policy

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

a) **Identification & Authentication**
The TOE requires all TOE users to identify and be authenticated.

b) **Access Control**
The backups and archives saved by a client node account to a server

are protected by an editable list of rules. By default only the Client Node account can access the data, a Client Node account can modify its list of rules.

c) **Secure Communications**
The TOE uses SSLv3/TLSv1 communications between distributed components of the TOE to protect the data, including TSF data, transferred between these components.

d) **Security Management**
The TOE supports privilege classes and client access authorities for administrative accounts allowing the administrative power of an administrator to be restricted to specific roles.

2.4 TOE Architecture

17 IBM Tivoli Storage Manager v5.5.1 employs a distributed client-server architecture. The major subsystems are identified in the Figure 2 - Schematic TOE component view and physical boundaries. The TOE consists of the following major architectural components:

a) Distributed client-server architecture

b) Backup/archive client:

i) command line (CLI)

ii) graphical interface

iii) web based interface

c) Client acceptor daemon (CAD)

d) Logical volume snapshot agent (optional)

e) Journal engine service – Windows only (optional)

f) Server system:

i) authentication

ii) authorisation

iii) TSM database server

iv) storage management

v) logging

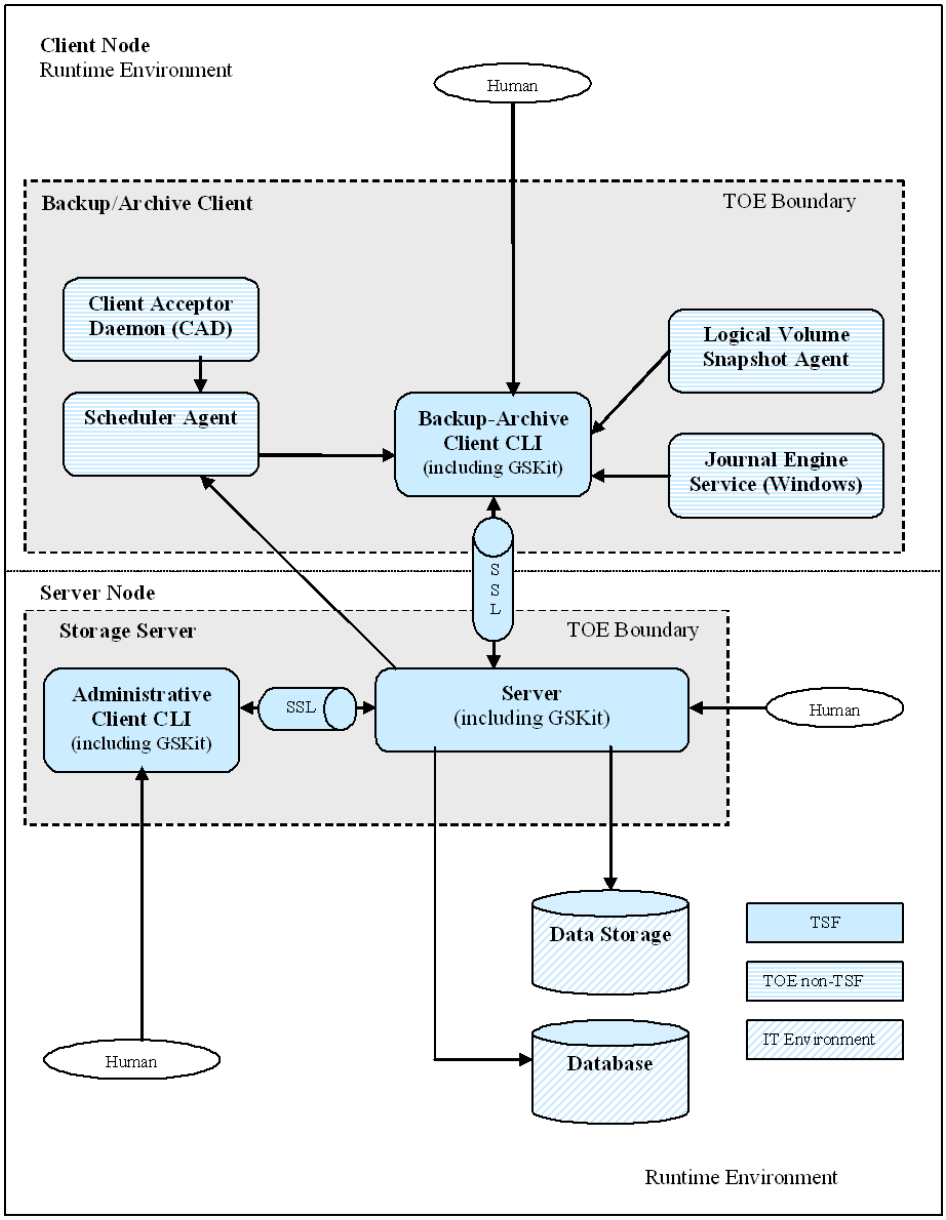

Figure 2 - Schematic TOE component view and physical boundaries.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

19 The evaluated configuration is detailed in the Security Target (Ref [1]) and the key policies that are applied to the TOE in the evaluated configuration are:

a) **Authenticate**
states the TOE must ensure that all users using client authentication who are not using the TSM server console, are identified and authenticated before being granted access to the TOE mediated resources.

b) **Privacy**
the TOE provides a mechanism to limit the scope of control of a given administrator.

c) **No bypass**
the security policy enforcement functions must be invoked and succeed before allowing access to TOE protected objects and functions.

d) **Confidentiality**
which states the TOE must protect backup, archive, and restore data from disclosure. The TOE must protect TSF data from disclosure.

e) **Secure defaults**
ensures that only secure values are used by administrators when managing the configuration of the cryptographic functions.

2.5.2 Non-evaluated Functionality

20 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 and Technology Security Manual (ISM) (Ref [2]) 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).

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

a) Network Data Management Protocol (NDMP) backup for NAS.

b) Automated disaster recovery planning with Disaster Recovery Manager.

c) Advanced tape library support: greater than 4 drives or 48 tape slots.

d) Library sharing

2.6 Usage

2.6.1 Evaluated Configuration

22 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 these defined evaluated configurations. Australian Government users should refer to the ISM (Ref [2]) to ensure that the configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

23 The TOE is comprised of the following software components:

a) The TOE is Tivoli Storage Manager v5.5.1. The evaluated configuration includes both the server component and the backup-archive client (BAClient) component.

b) Server components were tested on both Windows Server 2003 (32 bit Intel) and AIX5.3 (64 bit RISC). Windows Server 2003 (64 bit) is included in the evaluated configuration.

c) The BAClient component was tested on a WindowsXP SP3 machine. All three interface types were tested (command line, GUI and web based).

d) Default installations were performed in all tested cases.

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

2.6.2 Delivery procedures

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

25 In the evaluated configuration, the IBM Tivoli Storage Manager product is delivered electronically. Before placing an order, the customer must enrol online in IBM's Passport Advantage program. Customers enrol online using the following website: http://www-142.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/howtoenroll.

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

27 The customer must first obtain 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 Tivoli Storage Manager.

28 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.

29 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.

30 The TOE can initially be identified after download by the file name being one of the following zip files:

a) C17ANML.tar.gz - IBM TSM V5.5 AIX Server

b) C17ATML.tar.gz - IBM TSM V5.5 AIX clients

c) C17ASML.exe - IBM TSM V5.5 Windows Server

d) C17AZML.exe - IBM TSM V5.5 Windows IA64 Client

e) C17B0ML.exe - IBM TSM V5.5 Windows x32 Client

f) C17B1ML.exe - IBM TSM V5.5 Windows x64 Client

31 Once extracted, the TOE version is visible.

32 Obtaining the evaluated version 5.5.1, requires another download. After login to passport advantage, go to http://www-01.ibm.com/software/support

a) Choose "Tivoli" from the 1st pull down menu "navigate to a brand or product support"

b) If another pull down menu labelled “select a product” appears, choose “IBM Tivoli Storage Manager”

c) If another pull down menu doesn’t appear, click on the arrow following the “brand” pull down menu, then choose “IBM Tivoli Storage Manger” as the product.

d) When you get to the page entitled “IBM Tivoli Storage Manager Support”, choose “download” in the blue shaded box on the right side of the screen; and

e) A list of the latest updates appears. download ‘fix pack 1’.

2.6.3 Determining the Evaluated Configuration

33 The TOE is verified as part of the download process by Download Director. The user simply needs to verify the version number within the TOE.

2.6.4 Documentation

34 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available from the developer to ensure secure installation of the product:

a) Tivoli Storage Manager for AIX Version 5.5: Installation Guide (Ref [3])

b) Tivoli Storage Manager for UNIX and Linux Version 5.5: Backup-Archive Clients Installation and User's Guide (Ref [4])

c) Tivoli Storage Manager for Windows Version 5.5: Backup-Archive Clients Installation and User's Guide (Ref [5])

d) Tivoli Storage Manager for Windows Version 5.5: Installation Guide (Ref [6])

e) IBM Tivoli Storage Manager for AIX Version 5.5: Administrator's Reference (Ref [7])

f) IBM Tivoli Storage Manager for Windows Version 5.5: Administrator's Reference (Ref [8])

g) IBM Tivoli Storage Manager API Version 5.5: Tivoli Storage Manager Application Programming Interface Guide (Ref [9])

h) IBM Tivoli Storage Manager, Common Criteria Guide 5.5.1 (Ref [10])

2.6.5 Secure Usage

35 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.

a) The administrators are appropriately trained and trustworthy.

b) The TOE is physically secure.

c) The IT environment, including Certificate Authority (CA) (if it exists) and Network Time Protocol (NTP) services, is trustworthy.

d) The information flow policy for the TOE to enforce is valid.

Chapter 3 - Evaluation

3.1 Overview

36 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

37 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [11], [12], [13]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [14]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Ref [15], [16], [17], [18]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [19]) were also upheld.

3.3 Functional Testing

38 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.

39 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:

a) identification and authentication;

b) user and data protection;

c) security management;

d) protection of the TOE security functions.

3.4 Penetration Testing

40 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information.

41 The evaluators performed an independent vulnerability analysis using the developer's vulnerability analysis as well as their own (independent) search to devise and perform the following penetration tests:

a) idle timeout tests;

b) crypto component test;

c) system privilege test account lockout test;

d) secure crypto attribute test;

e) attribute test;

f) account initialisation test

42 and determined that:

a) the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP was described;

b) the disposition of obvious vulnerabilities was described; and

c) for all identified vulnerabilities, the vulnerability cannot be exploited in the intended environment for the TOE.

43 The TOE behaved as expected in each of the vulnerability tests. As such, no exploitable vulnerabilities were found.

Chapter 4 - Certification

4.1 Overview

44 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

45 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [20]), the ACA certifies the evaluation of IBM Tivoli Storage Manager v5.5.1 performed by the Australasian Information Security Evaluation Facility, stratsec.

46 stratsec has found that IBM Tivoli Storage Manager v5.5.1 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL3 augmented with ALC_FLR.1.

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

4.3 Assurance Level Information

48 EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behaviour.

49 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

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

51 ALC_FLR.1 provides basic flaw remediation: Flaw remediation requires that discovered security flaws be tracked and corrected by the developer.

4.4 Recommendations

52 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 the ISM (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

53 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that users and administrators note:

a) As the server console does not provide any authentication functionality, the evaluators recommend that the TOE be invoked as a service and managed via WMI when installed on a Windows 2003 Server host. If the TOE is invoked from a command line (thus spawning an open console) suitable access controls must be applied over remote desktop services to prevent unauthorised access to the server console.

b) Appropriate physical access controls should also be applied to prevent unauthorised access to the server console. Passwords used to access the TOE are not case sensitive and are limited to: any letter a-z upper or lower case, any number 0-9, the underscore, a period, a hyphen, a plus sign, or an ampersand. Due to these limitations on the set of characters allowed for passwords, the evaluators recommend that TOE administrators enforce suitable minimum password lengths and expiry periods in the TOE configuration. Customers should also incorporate a TOE specific password policy into the relevant organisational security policies.

c) The evaluators noted that TOE administrative client software (dsmadmc.exe) automatically re-establishes a terminated idle connection when the user next attempts to execute any functions. The user is not prompted to re-enter a password if the client software is not terminated prior to executing the administrative commands. The evaluators recommend that the administration console be installed on an appropriately secured machine.

d) Finally, the evaluators observed during testing that data being archived or backed up from the BA Client components is encrypted using AES with 128-bit key lengths. If 256-bit encryption is required, the data must be encrypted with a separate encryption utility prior to invoking a backup or archive operation.

Annex A - References and Abbreviations

A.1 References

[1] IBM Tivoli Storage Manager Version 5.5.1 Security Target Version 1.6.10, March 2009, IBM Corp.

[2] Australian Government Information and Communications Technology Security Manual (ISM), September 2008, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Tivoli Storage Manager for AIX Version 5.5: Installation Guide

[4] Tivoli Storage Manager for UNIX and Linux Version 5.5: Backup-Archive Clients Installation and User's Guide

[5] Tivoli Storage Manager for Windows Version 5.5: Backup-Archive Clients Installation and User's Guide

[6] Tivoli Storage Manager for Windows Version 5.5: Installation Guide

[7] IBM Tivoli Storage Manager for AIX Administrator's Guide version 5.5

[8] IBM Tivoli Storage Manager for Windows Version 5.5: Administrator's Reference

[9] IBM Tivoli Storage Manager API Version 5.5: Tivoli Storage Manager Application Programming Interface Guide

[10] IBM Tivoli Storage Manager v5.5.1 Common Criteria Guide

[11] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31

[12] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 2003-12-31

[13] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 2003-12-31

[14] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-12-31

[15] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.0, 21 February 2006, Defence Signals Directorate.

[16] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Defence Signals Directorate.

[17] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.0, 21 February 2006, Defence Signals Directorate

[18] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.0, 21 February 2006, Defence Signals Directorate

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

[20] Evaluation Technical Report for IBM Tivoli Storage Manager v5.5.1, May 2009.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
B/A	Backup/Archive
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
TSP	TOE Security Policy