122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP235

Citrix Password Manager, Enterprise Edition

Version 4.5

running on Microsoft Windows and Citrix Presentation Server

Issue 1.0

June 2007

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor	Citrix Systems, Incorporated
Product and Version	Citrix Password Manager, Enterprise Edition, Version 4.5
Description	The product is a single sign-on solution for accessing password-protected Windows, Web and host based applications.
CC Part 2	Conformant
CC Part 3	Conformant
EAL	EAL2 augmented by ALC_FLR.2
CLEF	BT
Date authorised	29 June 2007

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [e], CC Part 2 [f], CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

Trademarks:

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Citrix Password Manager, Enterprise Edition, Version 4.5, to the Sponsor, Citrix Systems Incorporated, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

   Citrix Password Manager, Enterprise Edition, Version 4.5.

4. The Developer was Citrix Systems, Incorporated.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE scope, its assumed environment and the evaluated configuration are given in Chapter III ‘Evaluated Configuration’ below.

6. The TOE provides a single sign-on solution for accessing password-protected Windows, Web and host-based applications. After a user has authenticated to the network using their primary credentials (this authentication is managed by the environment), all attempts to open controlled applications result in the TOE providing that user’s secondary credentials to the application.

7. An administrator is responsible for bringing an application under the TOE’s control (‘making a controlled application’) and for defining the Password Policy to be enforced for each application or group of applications. The administrator is also responsible for setting up a user’s initial Secondary Credentials for an application (‘provisioning’). In the evaluated configuration, a user is not exposed to his/her application passwords; those passwords are pre-populated by the administrator and managed and changed as required by the TOE. This means that a user cannot inadvertently or deliberately divulge his/her application passwords and also, as the user never enters an application password via the keyboard, those passwords cannot be detected via keyboard logging. It is possible for the administrator to re-provision a user by entering new provisioning data.

8. The evaluated configuration relies on users not having administrator level permissions for the operating system on which the product is evaluated. The evaluated configuration also relies on the machines (on which the server components are installed) being physically secure and accessed only by trusted

personnel. Additionally, the operating systems on which the TOE components are installed must have correctly installed certificates for use by Transport Layer Security (TLS) encryption services.

9. An overview of the product and its security architecture can be found in Chapter IV ‘Product Security Architecture’ below.

Protection Profile Conformance

10. **The Security Target [d] does not claim conformance to any protection profile**.

Security Claims

11. The Security Target [d] fully specifies the TOE’s security objectives, the threats which these objectives counter, the Organisational Security Policies (OSPs) which those objectives meet, and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

12. The TOE security policy (the Password Generation Policy) is detailed in Section 6.1 of the Security Target [d]. The OSP with which the TOE must comply is defined in Section 3.3 of the Security Target.

Strength of Function Claims

13. **The minimum Strength of Function (SoF) was SoF-Medium**. This was claimed for security function F3, Application Password Generation. **The Certification Body has determined that these claims were met.**

Evaluation Conduct

14. The Certification Body monitored the evaluation, which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in June 2007, were reported in the Evaluation Technical Report (ETR) [j].

Conclusions and Recommendations

15. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

16. **Prospective consumers of Citrix Password Manager, Enterprise Edition, Version 4.5, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

17. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III ‘Evaluated Configuration’ below.

18. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II ‘Product Security Guidance’ below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

19. **Certification is not a guarantee of freedom from security vulnerabilities**; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body’s view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

20. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

21. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery**.

22. The TOE is supplied via Federal Express, DHL or UPS. The shipping company used, the shipping tracking number and a description of the items shipped is emailed to the customer. Each order is assembled and an address label attached. The TOE CD-ROM is placed in a cardboard wallet with other information and shrink wrapped. The license details are placed in a tamper evident cardboard wallet. To verify secure delivery a customer should:

    a. check that the tamper evident packaging, containing the TOE, is intact;

    b. check that the courier company used and shipping tracking number of the delivered TOE are the same as those on the email sent to the customer.

    If any of these checks fail, the customer should contact Citrix Customer Service.

23. Customers are required to download a hotfix in order to install the Agent. The instructions for this are on Page 48 of the Evaluated Configuration Guide [i] (which is a PDF document dowloadable from www.citrix.com). The integrity of the download can be checked by performing an MD5 hash of the installation file (setup.msi) and comparing it to the value given in the Evaluated Configuration Guide [i] (233c33ead2b7abd566f95a66b93173ac).

Installation and Guidance Documentation

24. Procedures for secure installation, generation and start-up of the TOE are provided in the Evaluated Configuration Guide [i] and the Administrator’s Guide [k]. These documents should be read together before installing the TOE.

25. The guidance for administration and use of the TOE can be found in the Administrator’s Guide [k]. Note that all human interaction with the TOE is by authorised administrators and that user guidance is therefore not applicable.

III. EVALUATED CONFIGURATION

TOE Identification

26. The TOE consists of:

    a. one Citrix Password Manager Console version 4.5 Enterprise Edition;

    b. one Citrix Password Manager Service version 4.5 Enterprise Edition;

    c. one Citrix Password Manager Agent version 4.5 Enterprise Edition.

27. Those three items of software are all delivered on one CD-ROM labelled “Citrix Password Manager, Version 4.5”.

TOE Documentation

28. The relevant guidance documentation for the evaluated configuration is identified above under ‘Installation and Guidance Documentation’. The Administrator’s Guide [k] is on the same CD-ROM as the TOE software.

TOE Scope

29. The following features of Citrix Password Manager, Enterprise Edition, Version 4.5, are excluded from the scope of the evaluation:

    a. Key Recovery via Question-Based Authentication;

    b. Self-Service Password Reset using Question-Based Authentication;

    c. Account Unlock using Question-Based Authentication;

    d. Use of an NTFS Network Share on a Windows Server, as the Central Store;

    e. Use of a Shared Folder in a Novell Netware Directory Services Schema, as the Central Store;

    f. Hot Desktop;

    g. Initial Credential Setup by a User;

    h. Enhanced Java Support;

    i. Domain Credential Sharing Group.

TOE Configuration

30. The evaluated TOE configuration is as detailed in Section 2 of the Security Target [d]. The TOE can be operated in four configurations as follows:

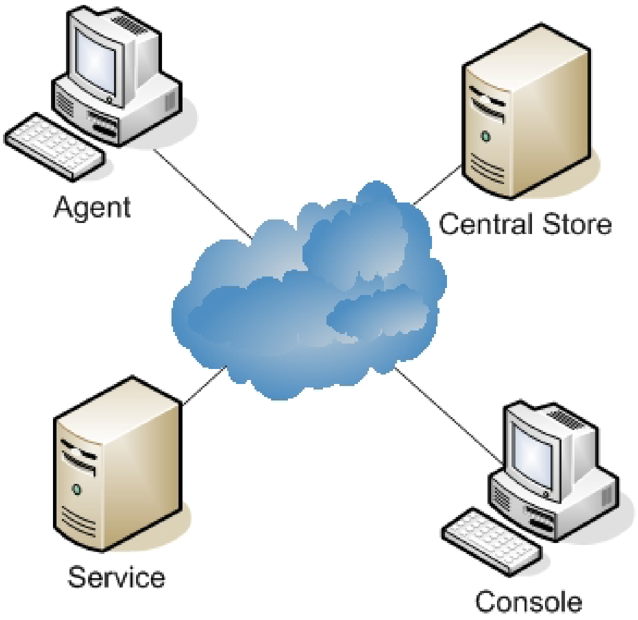

Diagram 1 – TOE in Stand Alone configuration with username and password authentication

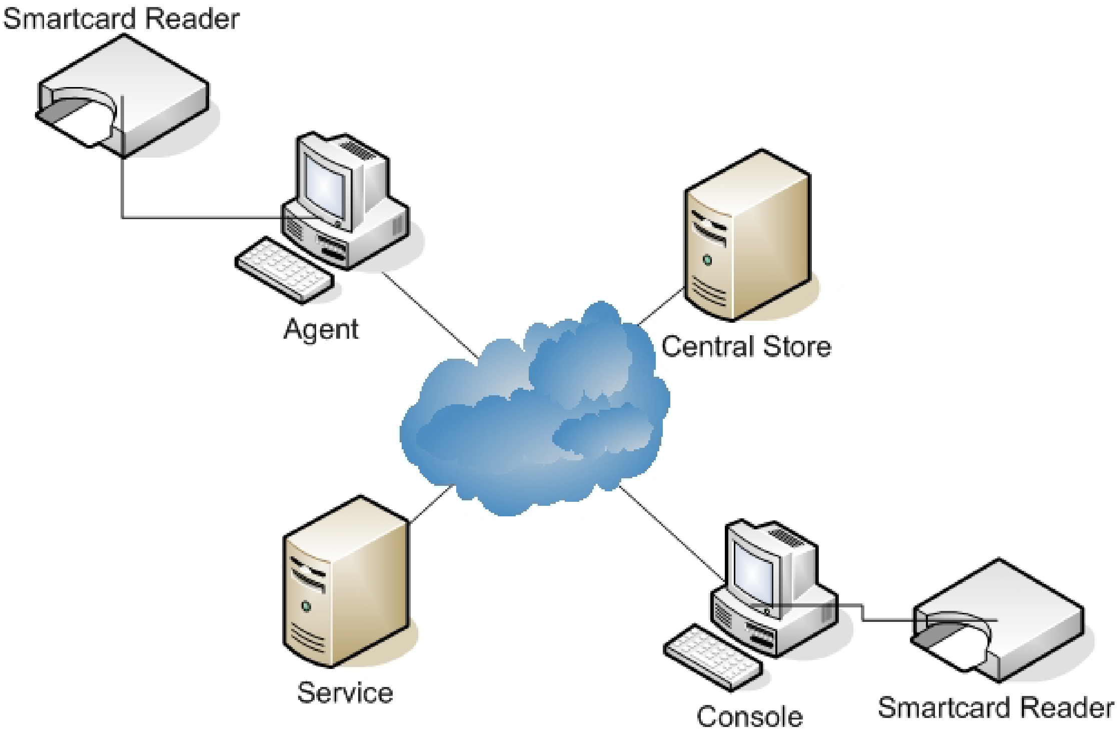

Diagram 2 – TOE in Stand Alone configuration with smartcard authentication

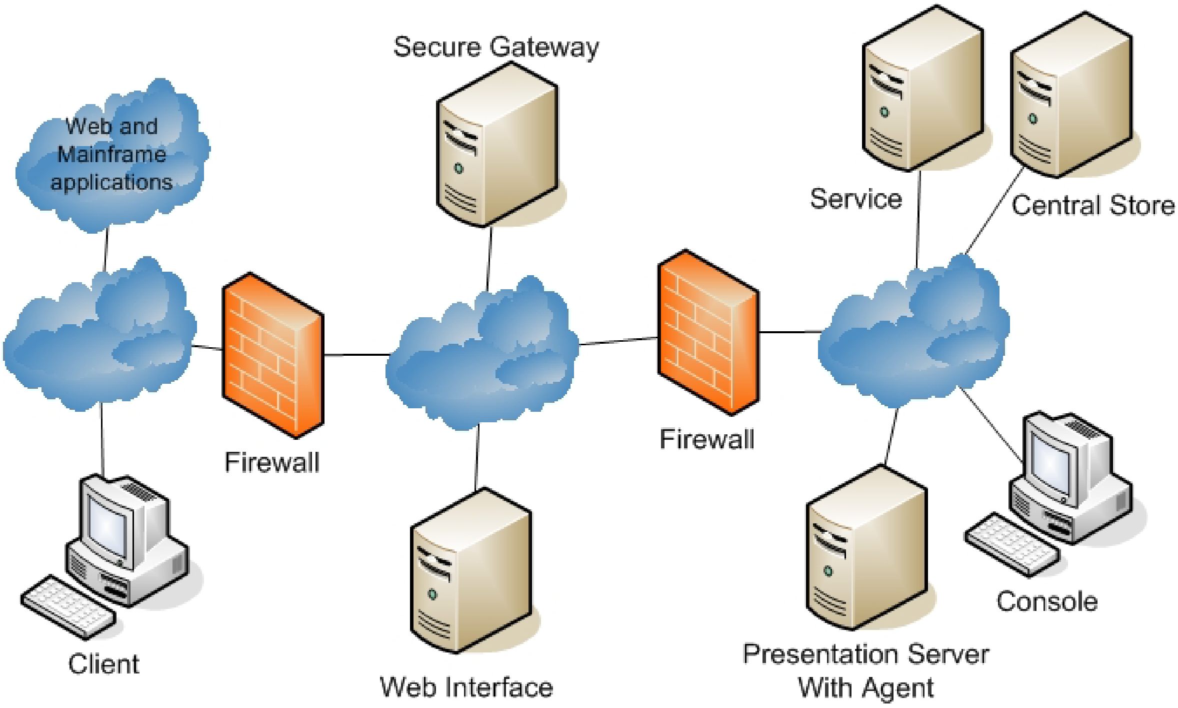

Diagram 3 – TOE in Citrix Presentation Server configuration with username and password authentication

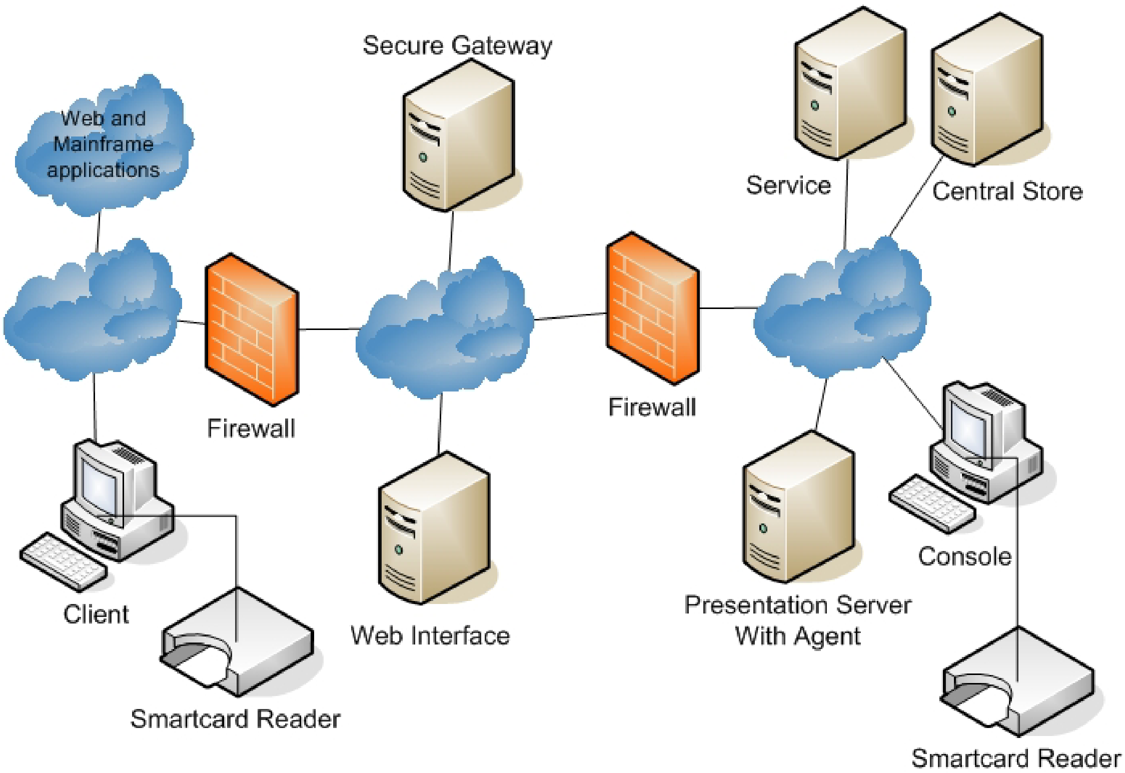

Diagram 4 – TOE in Citrix Presentation Server configuration with smartcard authentication

Environmental Requirements

31. The environmental configuration is as described in Sections 2.2, 2.3, 3.4 and 4.2 of the Security Target [d].

32. Figures 2-1 and 2-2 of the Security Target [d] show the TOE's essential interactions across the network. Diagrams 1 to 4 in Paragraph 30 above show, in outline, the position of the various platforms within the TOE's environment.

Test Configuration

33. The configuration in Diagram 4 of Paragraph 30 above was used for testing. The TOE was installed and configured according to the Evaluated Configuration Guide [i], referencing the Administrator's Guide [k] when necessary.

34. The Service Platform was an HP ProLiant DL140 with 2.4 GHz Xeon CPU, 1Gb RAM, 80Gb HDD and Intel Pro/100 NIC running Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1.

35. The Central Store, Web Interface and Secure Gateway Platforms were the same as the Service Platform, except that they had 512Mb RAM.

36. The two firewall platforms were the same as the Service Platform except they had 512Mb RAM, two Intel Ether Express/100 NICs and were running Red Hat 9 Linux.

37. The Client and Console platforms were both Dell PowerEdge SC1420 with 3.2 GHz Xeon CPU, 2Gb RAM, 80Gb HDD and Embedded Intel Gbit NIC running Microsoft Windows XP Professional with Service Pack 2. A GEMPC Smartcard Reader was attached to each machine via USB.

38. The Presentation Server with Agent platform was a Dell PowerEdge SC1420 with 3.2 GHz Xeon CPU, 2Gb RAM, 80Gb HDD and Embedded Intel Gbit NIC running Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1.

IV. PRODUCT SECURITY ARCHITECTURE

Introduction

39. This Chapter summarises the product's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

40. An overview of the TOE and the TOE architecture is provided in Sections 2.1 and 2.2 respectively of the Security Target [d].

41. Diagrams 1 to 4 in Paragraph 30 above show the various outline network topologies that are applicable to the TOE.

42. The TOE security policy (the Password Generation Policy) is detailed in Security Function F3 in Section 6.1 of the Security Target [d]. Specific parameter settings are detailed in the Evaluated Configuration Guide [i].

43. The main security protection mechanisms of the TOE are :

    a. Secure Password Use – the TOE generates strong passwords in accordance with a password policy and never discloses them to the user with whom they are associated;

    b. Secure Application Use – the TOE only submits identification and authentication credentials to verified Web and Windows applications;

    c. Cryptographic Security – the TOE uses cryptographic techniques to protect user and administrative data, both internally and by use of Windows encryption modules.

Design Subsystems

44. The subsystems of the Agent component are:

- SSOGina;
- Auth;
- Agent Crypto;
- Local Cache;
- Agent Thread;
- Password Generation;
- Sync.

45. The subsystems of the Service component are:

- Authenticator;
- Key Recovery Service;
- Data Integrity Service;
- Provisioning Service;
- Service Crypto.

46. The subsystems of the Console component are:

- Console;
- Console Crypto.

47. The subsystems and interfaces of the TOE are shown within the shaded boxes in Diagram 5 below:

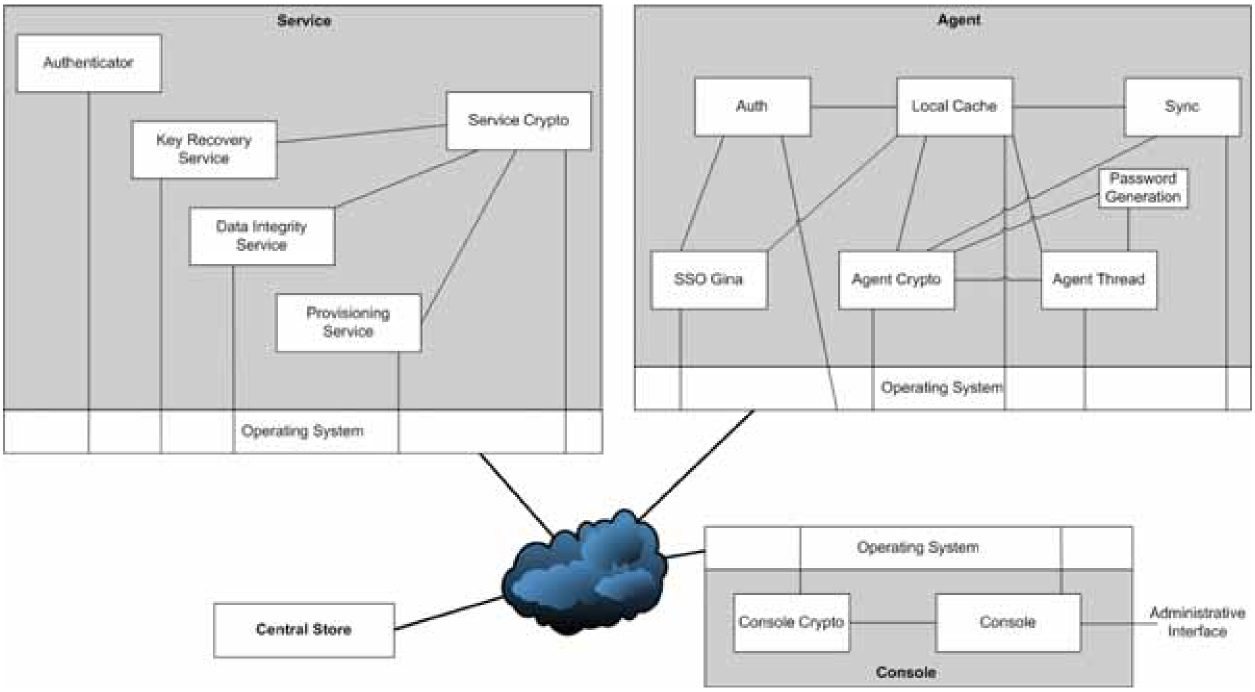

Diagram 5 – TOE Subsystems

Hardware and Firmware Dependencies

48. The TOE is a software-only TOE and is dependent on a Windows operating system to run. The TOE interacts with Windows through various Microsoft defined Application Programming Interfaces (APIs). The TOE requires Windows to be configured to use only FIPS 140 compliant encryption modules. This is stated in the Evaluated Configuration Guide [i].

Product Interfaces

49. The TOE consists of the following external interfaces:

a. Administrator’s interface into the TOE via the Console subsystem;

b. Interface between the TOE and the operating system.

V. PRODUCT TESTING

IT Product Testing

50. The Evaluators confirmed that the Developer's testing covered all security functions stated in the Security Target [d], and covered all subsystems and interfaces stated in Chapter IV 'Product Security Architecture' above.

51. The Evaluators performed independent functional testing on the TOE to confirm that it operates as specified. They also repeated a sample of 21% of the Developer's tests to confirm the adequacy of the Developer's testing of all of the TOE Security Functions (TSF), subsystems and TSF Interface (TSFI). The Evaluators performed this testing between April 30th and May 3rd 2007 at Citrix premises in Fort Lauderdale, Florida, USA.

52. The Evaluators then performed penetration testing, which confirmed the SoF claimed in the Security Target [d] for the password generation mechanism. That testing also confirmed that all identified potential vulnerabilities in the TOE have been addressed, i.e. that the TOE in its intended environment has no known exploitable vulnerabilities. The Evaluators performed this testing between April 30th and May 3rd 2007 at Citrix premises in Fort Lauderdale, Florida, USA.

53. The Evaluators used Brutus Release 2 tool (obtained from http://www.hoobie.net) during their testing. Other than that, no specialist tools or techniques were used.

Vulnerability Analysis

54. The Developer's vulnerability analysis describes the disposition of all known vulnerabilities relating to the TOE, as identified by design analysis and an extensive search of public domain sources of vulnerabilities.

55. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation process. The Evaluators confirmed that the Developer's vulnerability analysis was consistent with the Security Target [d] and with the countermeasures detailed in the Evaluated Configuration Guide [i] and the Administrator's Guide [k]. This analysis resulted in the identification of penetration tests, which were executed by the Evaluators. No exploitable vulnerabilities were identified.

Platform Issues

56. Details of the TOE scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' above.

57. The Developer provided evidence of testing the TOE on the evaluation platforms detailed in Paragraphs 33 to 38 above.

58. The Evaluators re-ran the Developer's test sample using the same configuration and equipment as the Developer.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[d] Security Target for Citrix Password Manager, Enterprise Edition, Version 4.5,
Citrix Systems, Inc,
Citrix Password Manager/ST, Version 1.0, 22 June 2007.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[i] Citrix Password Manager 4.5, Enterprise Edition, Common Criteria Evaluated Configuration Guide,
Citrix Systems, Inc,
9 May 2007.

[j] Evaluation Technical Report, Common Criteria EAL2 Evaluation of Citrix Password Manager 4.5, Enterprise Edition,
BT CLEF,
LFS/T508/ETR, Issue 1.0, June 2007.

[k] Citrix Password Manager Administrator's Guide,
Citrix Systems, Inc,
25 October 2006.

This page is intentionally blank