Security Target

for

Citrix Password Manager, Enterprise Edition, Version 4.5

Reference: Citrix Password Manager/ST

22 June 2007

Version: 1.0

This document has been prepared on behalf of:

Citrix Systems, Inc
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA

Prepared by:

BT
Aldershot AMTE
Ordnance Road
Aldershot
Hampshire, GU11 2AH
UK

DOCUMENT CONTROL

DOCUMENT TITLE	Security Target for Citrix Password Manager, Enterprise Edition, Version 4.5

Version	Date	Description
0.1	June 2006	Draft for certifier review
0.2	July 2006	Updated to address EOR 1
0.3	July 2006	Further updates in response to EOR 1
0.4	July 2006	Minor edits
0.5	September 2006	Updated to clarify FDP_RIP.1 claim
0.6	November 2006	Updated to clarify specifications of operating systems
0.7	April 2007	Updated to correct version of TOE in section 2.4.
1.0	June 2007	Updated following Certifier comments

Contents

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (ISO/IEC 15408 (1-3):2005)

GLOSSARY AND TERMS

Administrator	A person who is responsible for administering both the TOE and the environment. It is the administrator's responsibility to configure the administrative settings and services through the Console and to review the audit log on the Agent machines. Administrators must be identified and authenticated in the environment before performing any activities. Administrators have physical access to all machines that the components of the TOE (and the Active Directory) are installed on and are members of the Domain Administrative Group.
Administrative Data	Various settings controlled through the Console and stored in the Central Store. Within the scope of the evaluation these settings consist of: • Password Policies • Details of Users • Details of Controlled Applications (including which users have access to the application and whether the application requires Domain Re-Authentication)
Agent Software	The Agent Software intercepts an application's request for authentication and submits a user's Secondary Credentials.
Application Password	The user's password which is submitted by the TOE to a controlled application. The application password is either provisioned by the Administrator or generated by the TOE and never disclosed to the user.
Attacker	A person on the network whose credentials have not been provisioned by the Administrator and who has no legitimate access to any controlled applications.
CC	Common Criteria for Information Technology Security Evaluation
Central Store	The Password Manager Environmental component that stores Administrative Data for the TOE and user's secondary credentials. In the evaluated configuration this is a container in an Active Directory schema.
Citrix Password Manager Service	A component of the TOE providing Data Signing, Credential Provisioning and Automatic Key Recovery functionality.

Console	The Administration Management Tool used to control all aspects of the TOE.
Controlled Application	An application configured by an Administrator to work under the control of Password Manager. When a controlled application is launched the TOE submits the users' secondary credentials to that application.
IT	Information Technology
Object	An entity within the TSC that contains or receives information and upon which subjects perform actions.
Primary Credentials	The credentials used by a user to perform the initial logon to the domain.
Provisioning	The administrative act of adding initial usernames and passwords for a controlled application to the Central Store. It is also possible for the administrator to re-provision a user at a later time by adding new provisioning data.
Secondary Credentials	The credentials submitted by the TOE to all controlled applications.
ST	Security Target
Subject	An entity within the TSC that causes operations to be performed.
TLS	Secure Sockets Layer (SSL) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Transport Layer Security (TLS) is the latest, standardized version of the SSL protocol. TLS is an open standard and like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks. For the TOE, only use of TLS is within scope.
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSF Data	Administrative Data controlled through the Console and Secondary Credentials stored and transmitted by the TOE.
TSP	TOE Security Policy

User	A person who has legitimate access to one or more controlled applications.

1 Introduction to the Security Target

1.1 Security Target Identification

Document Title	Security Target for Citrix Password Manager, Enterprise Edition Version 4.5
Version	Version 1.0
Owner	Citrix Systems, Inc.
Originator	BT
TOE	Citrix Password Manager 4.5, Enterprise edition
CC Version	2.3, August 2005 [CC]
Assurance Level	EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures.

1.2 Security Target Overview

This document describes the security features of the Citrix Password Manager, Enterprise Edition, Version 4.5, (CPMe 4.5).

This Security Target includes the definition of the TOE, its scope and dependencies. It also lists the security requirements to be evaluated and how these are satisfied by the functionality of the TOE and/or associated policies.

1.3 CC Conformance Claim

This TOE makes the following conformance claims with respect to [CC]:

- Part 2 conformant.
- Part 3 conformant, EAL2 augmented, resulting from the selection of ALC_FLR.2 – Flaw Reporting Procedures.

2 TOE Description

2.1 Overview

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.

An administrator is responsible for bringing an application under the TOE's control (making a controlled application) and also 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 their application passwords, they 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 their application passwords and also, as the user never enters an application password via the keyboard they can't be detected via any form of keyboard logging. It is possible for the administrator to re-provision a user by entering new provisioning data.

The TOE records a number of security related events which are then written to the Windows Event Log. These events are then available to be viewed through the environment.

A user's primary authentication to the network is managed by the environment and can be a username and password (managed by Active Directory) or authentication via a smartcard implementation.

2.2 Evaluated Deployment

The following components make up the TOE:

- The Console – This is the administration tool used to control all aspects of the TOE. It is used to create application definitions (generating a controlled application), to initially add users and passwords (provisioning) and for setting and managing password policies. In the evaluated configuration the Console is installed on a dedicated machine running Windows XP Professional.

- The Citrix Password Manager Service – The Password Manager Service is a web service that allows for automatic key recovery and provisioning. The Password Manager Service is also responsible for ensuring all Administrative Data is cryptographically signed before they are sent to the central store.

- The Agent – The agent software acts as an intermediary between users and

applications that require authentication. When a user tries to access an application that requires authentication the Agent Software intercepts the application's request for authentication, finds the correct credentials and submits them to the application. These credentials are stored in encrypted form on the Central Store, with a local copy stored on the Agent Software as well. In the evaluated configuration two types of instantiations for the Agent Software are possible:

- An agent running on a workstation. In the evaluated configuration the desktop machine is running Windows XP Professional and is managed by an administrator. The administrator will install applications and configure the applications as 'managed applications'. When a user of this machine attempts to open an application the Agent will be responsible for submitting the correct credentials.

- An agent running on a Presentation Server. In the evaluated configuration the Presentation Server Machine is running Windows 2003 Server and is managed by an administrator. Users will access applications (also stored on the Presentation Server) from a client machine.

In addition a Central Store is required to store Administrative Data. This can be an NTFS network share on a Windows Server, a container in an Active Directory schema or a shared folder in a Novell Netware directory services schema. Only the Active Directory solution is used in the evaluated configuration. It should be noted that a Schema Extension in accordance with Microsoft Guidelines is required to use Active Directory during configuration. Also, in order for the product to work a License Server must be available. This could be installed on the Presentation Server (when the Agent is running on a Presentation Server) or on a separate dedicated machine (when the Agent is running on a workstation). Furthermore, in the evaluated configuration two Domain Controllers will be used, these machines will both run Windows 2003 Server and will both be running the Active Directory Service. All these components are part of the environment and do not constitute the TOE.

A user must be authenticated by the Domain Controller before attempting to access any Controlled Application. This logon is managed by the environment and can be a username / password combination or via a smartcard solution. Citrix Password Manager supports the use of PC/SC-based cryptographic smartcards. These cards provide for two-factor authentication (the card and pin number) which when used together log the user into the environment. In order to authenticate in the domain a user will be provided with either a standard Windows Username / Password combination, or be set-up to use a smartcard. The configuration of the primary authentication mechanism is part of the environment of the TOE.

When the Agent Software is running on a Workstation, the TOE comprises the sample environment as described in Figure 2-1 below[1].

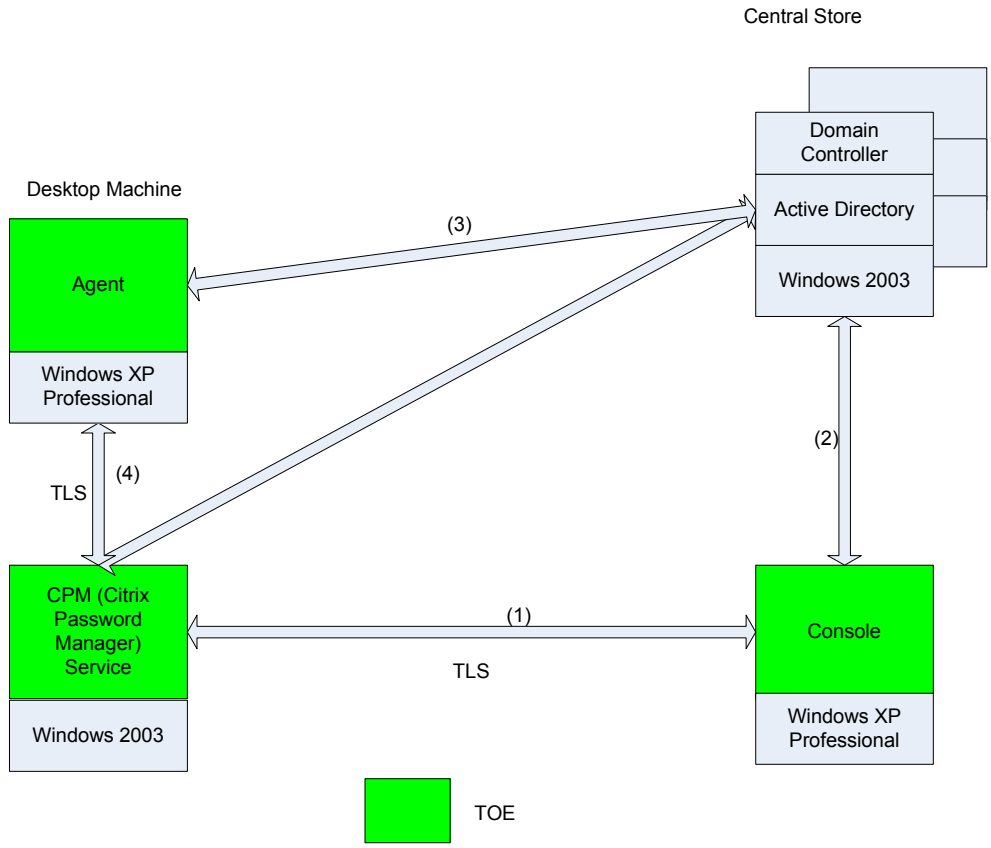

Figure 2-1 Evaluated Configuration

In addition it is also possible to install the Agent Software on a Citrix Presentation Server as shown in Figure 2-2 below[1].

[1] Figure 2-1 and 2-2 do not show interaction with the License Server. Although a License Server is required, it does not provide any security functionality within the evaluated configuration.

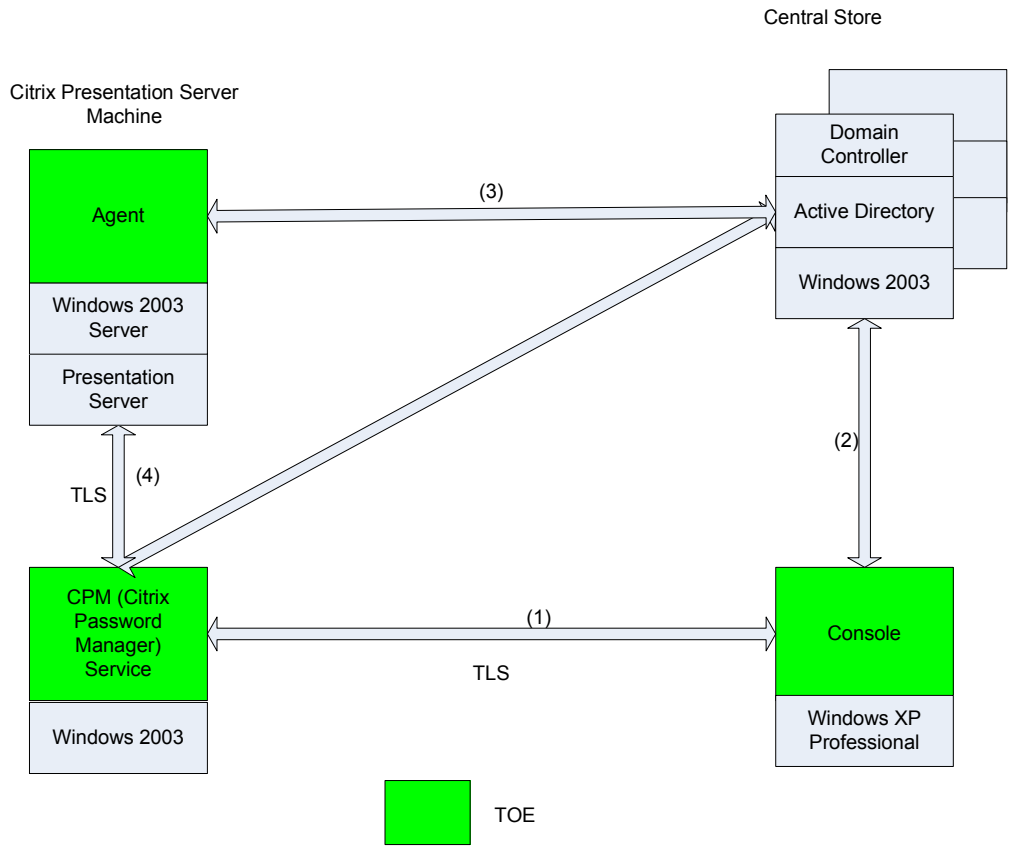

Figure 2-2 Agent Software running on Citrix Presentation Server

All other configurations of the TOE are outside the scope of the evaluation.

An administrator communicates with the TOE via the Console. The Administrative Data is then hashed and sent to the Citrix Password Manager Service via a TLS connection (1). The Citrix Password Manager Service digitally signs this data and sends it back to the console (1). The Console then communicates the digitally signed Administrative Data to the Central Store (2).

The Agent machine communicates with the Central Store in order to keep its local copy of the data up to date (3). The first time the Agent Software communicates with the Central Store, the Agent Software also requests the Certificate from the Citrix Password Manager Service (4). This is checked to ensure the integrity of the data received from the Central Store. The certificate is cached on the Agent machine and a further request for the Certificate is only made if the integrity check doesn't match or the Certificate has expired.

The Citrix Password Manager Service also communicates with the Central Store for a number of purposes:

- The Administrator is responsible for providing a user's initial application passwords. These passwords are entered through the Console which then sends them to the Password Manager Service. The Password Manager Service encrypts the passwords and sends the encrypted passwords to the Central Store.

- The first time a user logs in (on the Agent), the initial application passwords are transferred back from the Central Store to the Password Manager Service, decrypted and passed to the Agent.

- The interface between the Password Manager Service and the Central Store is also used during Key Recovery operations. As part of generating a Recovery Key the Password Manager Service stores an encrypted random data value in the Central Store. If Key Recovery is necessary this encrypted data is retrieved from the store and used to generate the Key Recovery Key.

All communication between TOE components is encrypted using TLS and thus there is no requirement for the Console the Citrix Password Manager Service and the Agent to be on a physically protected LAN. Data passed over the unprotected links to the Central Store is either encrypted (in the case of Secondary Credentials) or digitally signed (in the case of Administrative Data). The Central Store holds Secondary Credentials in encrypted form and Administrative Data in their signed form.

A user will access the Desktop machine directly, however for the Agent Software installed on the Presentation Server, a user will access this machine via a Citrix client. For simplicity this is not shown on the diagrams.

2.3 TOE Installation Requirements

2.3.1 Console Requirements

The Console is supported on Microsoft Windows XP Professional Service Pack 2 (or later), 32 bit version, with Microsoft .NET Framework 2.0 installed. Microsoft Windows Installer 3.0 is also required.

The minimum specification for the hardware platform should be a 233MHz Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.2 Citrix Password Manager Service Requirements

The Citrix Password Manager Service is supported on Microsoft Windows 2003 Server, Service Pack 1 (or later), 32 bit version, with Microsoft .NET Framework 2.0 installed.

The minimum specification for the hardware should be a 550MHz Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.3 Desktop Agent Requirements

The Agent installed on the workstation is supported on Microsoft Windows XP Professional Service Pack 2 (or later), 32 bit version. Microsoft Windows Installer 3.0 is also required.

The minimum specification for the hardware platform should be a 233MHz Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.4 Presentation Agent Requirements

The Agent installed on the Presentation Server machine is supported on Microsoft Windows 2003 Server with Terminal Services, Service Pack 1 (or later), 32 bit version and Microsoft Internet Information Services version 6.0 installed.

In addition Citrix Presentation Server Version 4.0 should be running.

The minimum specification for the hardware should be a 550MHz Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.5 Central Store Requirements

In the evaluated configuration the Central Store, acting as both a Domain Controller and an Active Directory Server is supported on Microsoft Windows 2003 Server, Service Pack 1 (or later), 32 bit version.

The minimum specification for the hardware should be a 550MHz Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.6 License Server Requirements

In the evaluated configuration a License Sever should be installed on the Presentation Server (if one is being used) or an a dedicated machine if the Agent is running on a desktop machine.

The 'Getting Started with Citrix Licensing Guide' provides details about the hardware and software requirements for a License Server.

2.3.7 Supported Hardware in IT Environment

Details of the hardware supported for Windows 2003 can be found on Microsoft's Server Catalog at http://www.microsoft.com/windows/catalog/server/.

Details of the hardware supported for Windows XP Professional can be found on Microsoft's catalog at http://www.microsoft.com/windows/catalog/.

2.4 Scope of TOE

The Target of Evaluation (TOE) will be the following components of Citrix

Password Manager 4.5, Enterprise Edition:

- One Citrix Password Manager Console version 4.5 Enterprise Edition
- One Citrix Password Manager Service version 4.5 Enterprise Edition
- One Citrix Password Manager Agent version 4.5, Enterprise Edition.

2.5 Excluded Components

The following Citrix Password Manager 4.5, Enterprise edition product components / functions are excluded from the scope of the evaluation:

- Key Recovery via Question-Based Authentication
- Self-Service Password Reset using Question-Based Authentication
- Account unlock using Question-Based Authentication
- Use of an NTFS Network Share on a Windows Server, as the Central Store
- Use of a shared folder in a Novell Netware Directory Services Schema, as the Central Store
- Hot Desktop
- Initial Credential Setup by a User
- Enhanced Java Support
- Domain Credential Sharing Group..

3 Security Environment

3.1 Introduction

This section provides the statement of the TOE security environment, which identifies and explains all:

- known and presumed threats countered by either the TOE or by the security environment;
- organizational security policies with which the TOE must comply;
- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Assets

- Administrative data that enable access to a controlled application, stored on, or in transit between TOE components.
- Secondary Credentials stored on, or in transit between, TOE components.
- TOE hardware.

3.2.2 Threat agent

The following are threat agents for the TOE:

Attacker	A person on the network whose credentials have not been provisioned by the Administrator and who has no legitimate access to any controlled applications.
User	A person who has legitimate access to one or more controlled applications. In this case, the threat would come from an authenticated user attempting access not granted to them.

3.2.3 Threats countered by the TOE

The following specific threats are countered by the TOE (in some cases with support from the environment):

T.USER	A user may inadvertently or intentionally divulge their application authentication credentials to another user or attacker.
T.STRENGTH	A user's application authentication credentials are easily guessable by an attacker.
T.ATTACK	An attacker may gain unauthorised access to a controlled application or to TOE data.
T.ACCESS	A user may gain unauthorised access to a controlled application or to TOE data.
T.WALKAWAY	A logged-in user may leave a session unattended without logging out, which could enable another user or an attacker to gain access to a controlled application.
T.PHISHING	An attacker could attempt to access a user's application authentication credentials by running an unauthorized copy of a controlled application.

3.2.4 Threats countered by the Operating Environment

The following threats are required to be countered by technical and/or non-technical measures in the IT environment:

T.MOD_HW	Unauthorised persons may gain access to the machine on which TOE components are installed.
T.MOD_STORE	Unauthorised persons may gain access to the machine on which the Domain Controller and Central Store are installed.
T.AUDIT_REVIEW	Audit Records may not be reviewed and examined

3.3 Organizational Security Policies

OSP.CRYPTO	Cryptographic functions shall be validated to FIPS 140-1 Level 1 or FIPS 140-2 Level 1.

3.4 Assumptions

A.FIPS	The Windows 2003 Server and Windows XP Professional Operating Systems must be configured in a FIPS 140-compliant mode.
A.TRUSTADMIN	Administrators are trustworthy.

A.DESKTOP	Where the Agent Software is installed on a desktop machine, users have no administrative rights over that machine and the configuration is assumed to be locked-down.
A.PHYSICAL	The machines hosting the Citrix Password Manager Service, the Console and the Central Stores are assumed to be physically protected. In addition if the Agent software is installed on a Citrix Presentation Server, this machine is also assumed to be physically protected.
A. APPLICATION	The controlled applications are trusted not to expose passwords to users.
A.THIRD_PARTY_ SW	Trusted third party software is operating correctly and securely. Trusted third party software is defined as: • Windows Server 2003 (including Active Directory) • Windows XP Professional • Citrix Presentation Server version 4.0 • Microsoft IIS (installed on the Presentation Server Agent).
A.SMARTCARD	Where a smart card is used, it will be tamper resistant and maintain the confidentiality and integrity private keys contained within it.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

The specific IT security objectives are as follows:

OT.CONF	The confidentiality of user application authentication credentials must be maintained during processing and transmission between TOE components.
OT.INTEG	The integrity of Administrative Data must be maintained during processing and transmission between TOE components and between the TOE components and the Central Store.
OT.APPLICATION	When an attempt is made by a user to open a controlled application, the credentials required to login to that application will be provided by the TOE.
OT.STRENGTH	In response to a password change request from a controlled application the TOE will generate application passwords in accordance with a defined policy.
OT.RE-AUTHN	For certain applications the Administrator shall be able to require the user to perform a domain re-authentication
OT.TIMEOUT	When a configurable time period has elapsed the TOE shall require the user to perform a domain re-authentication before performing any action with the TOE[2].
OT.PASSWORD	The TOE will not expose valid application passwords to any user (including the user of the credentials himself)
OT.PHISHING	The TOE will only submit application authentication credentials to the correct application.
OT.AUDIT	The TOE shall generate audit logs relating to the TOE changing and submitting application authentication credentials to a controlled application.

[2] This time period relates to the time since the user last performed a Domain Authentication and is not related to inactivity timeouts.

4.2 Environment Security Objectives

4.2.1 IT environment security objectives

The following IT security objectives are to be satisfied by the environment:

OE.THIRD_PARTY	Trusted third party software must be securely configured. Trusted third party software is defined as: • Windows Server 2003 (including Active Directory) • Windows XP Professional • Citrix Presentation Server version 4.0 • Microsoft IIS (installed on the Presentation Server Agent)
OE.SECURE_ ENCRYPTION	Secure encryption modules must be FIPS140-1 Level 1 (for Windows XP Professional) or FIPS 140-2 Level 1 (for Windows 2003 Server) compliant. Note – The operating systems used must be configured such that only FIPS140 implemented algorithms are used. The secure encryption module used within Microsoft Windows XP Professional has only been evaluated to FIPS140-1 Level 1. Thus within the ST it is necessary to claim compliance to both FIPS140-1 Level 1 (for Windows XP Professional) and FIPS140-2 Level 1 (for Windows 2003 Server). This objective will be met through correct use of services provided by a correctly configured operating system.
OE.SESSION_KEYS	Cryptographic session keys used for TLS encryption must be securely administered and protected from disclosure. Note – Session keys are managed entirely by the operating system as part of the TLS implementation. The TOE does not import or process these keys.
OE.AUDIT_REVIEW	Audit data must be available to be read and examined by an administrator.

4.2.2 Non-IT environment security objectives

Non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE software. Thus they will be implemented largely through procedural or administrative measures.

OE.PHYSICAL	Hardware running the following must be physically protected: • Console Machine • Citrix Password Manager Service Machine • Central Store Machines.
OE.DESKTOP	The machine running the Agent Software should be locked-down so that users have no administrative rights over that machine.
OE.CERTIFICATES	Certificate private keys must be accessible only by administrators. They must be obtained and maintained securely. This needs to be done at product installation and as determined by the relevant certification authority thereafter.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The TOE security functional requirements are presented in this section. Completed operations are shown in *italics*. Assignment and selection operations are encased in square brackets [], refinement operations are encased in angular brackets <> and iterations are indicated by use of (n) following the component designator, where n is the number of the iteration.

All components are taken from Part 2 of the CC.

Functional Components	
	Password Generation
FIA_SOS.2	FIA_SOS.2.1 – The TSF shall provide a mechanism to generate secrets that meet [*the administrator defined password policy for application passwords generated by the TOE*]. FIA_SOS.2.2 – The TSF shall be able to enforce the use of TSF generated secrets for [*all controlled applications*].
	Application Identification and Authentication
FIA_UID.2 (1)[3]	FIA_UID.2.1 – The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.2 (1)[3]	FIA_UAU.2.1 - The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[3] When an application starts the TOE will examine the login screen and submit the logged on user's application credentials (username and password) to a controlled application logon screen only if the user is permitted to access that application. Before submitting the application credentials the TOE also validates Windows Applications by using Secure Application ID Path Matching and Web Applications by using Secure URL Matching.

Functional Components	
	Domain Re-Authentication
FIA_UAU.6 (1)[4]	FIA_UAU.6.1 – The TSF shall re-authenticate the user under the conditions [1 *upon any attempt by a user to open a controlled application which requires 'domain re-authentication' as configured by the administrator* *2 upon any attempt by a user to open a controlled application when a configurable (by the administrator) time period has expired*].
	Cryptographic operation
FCS_COP.1(1)[5]	FCS_COP.1.1 – The TSF shall perform [*encryption of secondary credentials*] in accordance with a specified cryptographic algorithm [*3DES – with unique keys per user*] and cryptographic key sizes [192 bit] that meet the following • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*]
FCS_COP.1 (2) [5]	FCS_COP.1.1 – The TSF shall perform [*Cryptographic Data Signing of Administrative Data*] in accordance with a specified cryptographic algorithm [RSA with SHA-1] and cryptographic key sizes [1024] that meet the following • [*FIPS140-2 Level 1 on Windows 2003 Server*].

[4] This SFR is provided by both the TOE and the Environment. The TOE is responsible for assessing whether 'domain re-authentication' is required (based on administrative settings) however the actual re-authentication is performed by the Environment.

[5] These requirements are met partially by the TOE and partially by the environment. The TOE makes calls into the Operating System's Cryptographic library in order to generate keys, destroy keys and perform encryption and data signing. The actual cryptographic operations are performed by the Cryptographic Module within the Operating System

Functional Components	
FCS_COP.1(3)[6] Cryptographic operation	FCS_COP.1.1 – The TSF shall perform [*network encryption of secondary credentials and Administrative Data*] in accordance with a specified cryptographic algorithm [*3DES, as defined by the ciphersuite RSA_WITH_3DES_EDE_CBC_SHA in the TLS specification in RFC 2246*] and cryptographic key sizes [192 *bit*] that meet the following: • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*] Note: TLS_RSA_WITH_3DES_EDE_CBC_SHA has the following attributes: • Key Exchange = RSA • Cipher algorithm =3DES_EDE_CBC • Hash algorithm = SHA Further details can be found at "http://www.faqs.org/rfcs/rfc2246.html"
FCS_CKM.1 (1) [5] Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys <*the protection keys for the encryption of secondary credentials*> in accordance with a specified cryptographic key generation algorithm [*SHA1 hash as input to CryptDeriveKey*[7]] and specified cryptographic key sizes [*192 bit*] that meet the following [*FIPS140-1 Level 1 on Windows XP Professional* *FIPS140-2 Level 1 on Windows 2003 Server*].

[6] This requirement is met partially by the TOE and partially by the operating system in the environment. The TOE shall be configured to make use and request TLS encryption, however the actual encryption, including Key Management, is handled by the environment.

[7] CryptDeriveKey is the Microsoft Windows API that is called by the TOE in order to generate a cryptographic key.

Functional Components	
FCS_CKM.1 (2) [5] Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys <*the public / private key pair used for the cryptographic data signing of Administrative Data*> in accordance with a specified cryptographic key generation algorithm [CryptGenKey[8]] and specified cryptographic key sizes [*1024 bit*] that meet the following [*FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.4 (1) [5] Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys <*the protection keys for the encryption of secondary credentials*> in accordance with a specified key destruction method [*CryptDestroyKey*[9]] that meets the following [*FIPS140-1 Level 1 on Windows XP Professional* *FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.4 (2) [5] Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys <*the public / private key pair used for the cryptographic data signing of Administrative Data*> in accordance with a specified key destruction method [*CryptDestroyKey*[9]] that meets the following [*FIPS140-2 Level 1 on Windows 2003 Server*].
	Specification of Management Functions
FMT_SMF.1 Specification of Management Functions	FMT_SMF.1.1 - The TSF shall be capable of performing the following security management functions: *[* *a) Configuration of password policy to meet the defined Strength of Function* *b) The ability to define a controlled application* *c) The ability to add, modify and delete a users' initial application credentials from the Central Store*

[8] In line with FIPS PUB 186-2 Appendix 3 Random Number Generation.

[9] CryptDestroyKey is the Microsoft Windows API that is called by the TOE in order to destroy a cryptographic key.

Functional Components	
	(Provisioning) *d) The ability to selectively force domain re-authentication on the basis of certain controlled applications* *e) The ability to set a time period after which domain re-authentication will be required.]*
	Protection of the TSF
FPT_ITT.1 (1) Basic Internal TSF Data Transfer Protection	FPT_ITT.1.1 – The TSF shall protect TSF data <*secondary credentials*> from [*disclosure and modification*] when transmitted between separated parts of the TOE.
FPT_ITT.1 (2) Basic Internal TSF Data Transfer Protection	FPT_ITT.1.1 - The TSF shall protect TSF data <*Administrative Data*> from [*modification*] when transmitted between separated parts of the TOE.
	Reference Mediation
FPT_RVM.1 Non-bypassability of the TSP	FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSF is allowed to proceed Application Note The fact that the TOE must ensure that the TLS protocol is not bypassed during communication between TOE components is included by this SFR as is the submission of Secondary Credentials by the TOE upon each attempt to open a controlled application.
	Residual Information Protection
FDP_RIP.1 Subset residual information	FDP_RIP.1.1 – The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] the following objects [*memory on the Agent machine holding in the clear cryptographic key material and application*

Functional Components	
protection.	*passwords*].
	Audit
FAU_GEN.1	FAU_GEN.1.1 – The TSF shall be able to generate an audit record of the following audit events: a) Start-up and shutdown of the audit function; b) All auditable events for the [*not specified*] level of audit; and c) [*All successful and unsuccessful attempts to submit secondary credentials to a controlled application and all changes to users' application passwords by the TOE in response to a password change request from a controlled application*]. FAU_GEN.1.2 – The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

Table 5-1 Functional Requirements for the TOE

5.2 IT Environment Security Functional Requirements

The security functional requirements for the IT environment are presented in this section. The following table identifies those security requirements.

Functional Components	
	Cryptographic Key Management
FCS_CKM.1 (3) Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys <*the protection keys for the encryption of secondary credentials*> in accordance with a specified cryptographic key generation algorithm [*SHA1 hash as input to CryptDeriveKey*] and specified cryptographic key sizes

Functional Components	
	[*192 bit*] that meet the following • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.1 (4) Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys <*the public / private key pair used for the cryptographic data signing of Administrative Data*> in accordance with a specified cryptographic key generation algorithm [CryptGenKey[10]] and specified cryptographic key sizes [*1024 bit*] that meet the following • [*FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.1 (5) Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys <keys used *for the network encryption of secondary credentials and Administrative Data over TLS*> in accordance with a specified cryptographic key generation algorithm [*FIPS 186-2 Appendix 3 Section 3.3 SHS random number generator*] and specified cryptographic key sizes [192 *bit*] that meet the following: • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.2 (1) Cryptographic key distribution	FCS_CKM.2.1 – The TSF shall distribute cryptographic keys <*for the network encryption of secondary credentials and Administrative Data*> in accordance with a specified key distribution method [*RSA, as defined by the ciphersuite RSA_WITH_3DES_CBC_SHA in the TLS specification in RFC 2246*] that meets the following: • [*FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.4 (3) Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys <*the protection keys for the encryption of secondary credentials*> in accordance with a specified key destruction method [*CryptDestroyKey*] that meets the following

[10] In line with FIPS PUB 186-2 Appendix 3 Random Number Generation

Functional Components	
	• [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.4 (4) Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys <*the public / private key pair used for the cryptographic data signing of Administrative Data*> in accordance with a specified key destruction method [*CryptDestroyKey*] that meets the following • [*FIPS140-2 Level 1 on Windows 2003 Server*].
FCS_CKM.4 (5) Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys <*for the network encryption of secondary credentials and Administrative Data*> in accordance with a specified key destruction method [*TLS - Microsoft Schannel key destruction method*] that meets the following: • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*].
	Cryptographic operation
FCS_COP.1 (4) Cryptographic operation	FCS_COP.1.1 – The TSF shall perform [*encryption of secondary credentials*] in accordance with a specified cryptographic algorithm [*3DES – with unique keys per user*] and cryptographic key sizes [*192 bit*] that meet the following • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*]
FCS_COP.1 (5) Cryptographic operation	FCS_COP.1.1 – The TSF shall perform [*Cryptographic Data Signing of Administrative Data*] in accordance with a specified cryptographic algorithm [*RSA with SHA-1*] and cryptographic key sizes [*1024 bit*] that meet the following • [*FIPS 140-2 Level 1 on Windows 2003 Server*].
FCS_COP.1 (6) Cryptographic	FCS_COP.1.1 – The TSF shall perform [*network encryption of secondary credentials and Administrative Data*] in accordance with a specified cryptographic algorithm [*3DES,*

Functional Components	
operation	*as defined by the ciphersuite RSA_WITH_3DES_EDE_CBC_SHA in the TLS specification in RFC 2246*] and cryptographic key sizes [*192 bit*] that meet the following: • [*FIPS140-1 Level 1 on Windows XP Professional* • *FIPS140-2 Level 1 on Windows 2003 Server*] Note: RSA_WITH_3DES_EDE_CBC_SHA has the following attributes: • Key Exchange = RSA • Cipher algorithm =3DES_EDE_CBC • Hash algorithm = SHA Further details can be found at "http://www.faqs.org/rfcs/rfc2246.html"
	Identification and Authentication
FIA_UID.2 (2) User Identification before any action	FIA_UID.2.1 – The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. Note: This SFR applies to users who must be identified and authenticated within the environment before attempting to access any controlled application.
FIA_UAU.2 (2) User authentication before any action	FIA_UAU.2.1 – The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Note: This SFR applies to users who must be identified and authenticated within the environment before attempting to access any controlled application.

Functional Components	
FIA_UAU.6 (2)	FIA_UAU.6.1 – The TSF shall re-authenticate the user under the conditions [1 *upon any attempt by a user to open a controlled application which requires 'domain re-authentication' as configured by the administrator* *2 upon any attempt by a user to open a controlled application when a configurable (by the administrator) time period has expired*].
FIA_UID.2 (3) User Identification before any action	FIA_UID.2.1 – The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. Note: This SFR applies to administrators who must be identified and authenticated within the environment before attempting to perform any administrative actions through the console.
FIA_UAU.2 (3) User authentication before any action	FIA_UAU.2.1 – The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Note: This SFR applies to administrators who must be identified and authenticated within the environment before attempting to perform any administrative actions through the console.
	Domain Separation
FPT_SEP.1 TSF Domain Separation	FPT_SEP.1.1 – The TSF shall maintain a security domain for its own execution that protects it from interference and tampering from untrusted subjects. FPT_SEP.1.2 – The TSF shall enforce separation between the security domains of subjects in the TSC.
	Audit

Functional Components	
FAU_SAR.1	FAU_SAR.1.1 – The TSF shall provide [*an administrator*] with the capability to read [*audit data*] from the audit records. FAU_SAR.1.2 – The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FPT_STM.1	FPT_STM.1.1 – The TSF shall be able to provide reliable time stamps for its own use.

Table 5-2: IT Environmental Security Functional Requirements

5.3 TOE Security Assurance Requirements

The security assurance requirements are taken from Part 3 of the CC and are those that comprise the EAL2 assurance package, with the addition of ALC_FLR.2 Flaw Reporting Procedures). The assurance components are identified in the following table.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items document
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Flaw Remediation	ALC_FLR.2	Flaw Reporting Procedures
	ATE_COV.1	Evidence of coverage

Assurance Class	Assurance Components	
Tests	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-3: Assurance Requirements: EAL2 + ALC_FLR.2

Further information on these assurance components can be found in [CC] Part 3.

5.4 Strength of Function Claim

A Strength of Function (SoF) claim of SoF-Medium is made for the TOE. This SoF claim relates to the TSF's ability to generate a user's application passwords in accordance with the password policy set by an administrator (FIA_SOS.2). The administrator must follow guidance provided when setting the password policy to ensure that passwords of a sufficient strength are generated.

Note: The Windows operating system also provides a function that authenticates users. This is functionality provided by the TOE Environment and is thus not a mechanism requiring assessment.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in Section 5.1.

F1 – Application Definition

The Administrator must configure a controlled application before it can be accessed by a user.

F2 – Provisioning

The administrator shall be able to add, modify and delete a user's initial application credentials from the central store.

F3 – Application Password Generation

The TOE will generate application passwords in accordance with the password Policy as defined by an administrator.[11]

Application Note – The TOE allows the Administrator to define the following parameters as part of the Password Policy:

- Password Length;
- Character Repetition;
- Inclusion of lowercase alphabetic characters;
- Inclusion of uppercase alphabetic characters;
- Case sensitivity for first character;
- Inclusion of numeric characters;
- Inclusion of special characters;
- Exclusion of certain words, word fragment or characters;
- Exclusion of usernames;
- Password History;

[11] An explicit Strength of Function claim of SOF-Medium is made for this function.

- Password Expiration.

F4 – Secondary Credential Protection

The TOE will prevent the disclosure or modification of application passwords by any user (including the user to whom the credentials belong).

Application Note – In the evaluated configuration, a user will never know what their application passwords are. Application passwords are protected at enrollment (provisioning), during submission of an application password to a controlled application and during password change events. This means that a user cannot divulge their application passwords to other users and attackers and, as they are never entered via a keyboard, it will not be possible for an attacker to capture these passwords by keyboard logging or other such techniques.

F5 – Application Management

The TOE will examine all starting applications and will examine all existing Windows (associated with Windows and Web Applications) on Agent Startup. It will submit the logged in user's secondary credentials to a controlled application login screen only if that user is permitted to access the application. In addition, the TOE will validate Web Applications by using Strict URL Matching and Windows applications by using Secure ID Path Matching. In the case of Mainframe applications, due to their bespoke nature, no additional validation is performed.

Application Note – This function, combined with data signing of Administrative Data, ensures that an attacker cannot attempt to capture a user's secondary credentials by attempting to get the TOE to submit credentials to a spoofed controlled application.

F6 – Secondary Credential Encryption

All Secondary Credentials stored by the TOE are encrypted using 3DES encryption and unique keys for each user.

Application Note – The TOE uses Triple DES encryption in order to protect all Secondary Credentials. The TOE makes calls into Microsoft's Cryptographic Library in order to generate keys and perform encryption.

F7 – Administrative Data Integrity

All Administrative Data is digitally signed using RSA with SHA-1.

Application Note – The Password Manager Service digitally signs all Administrative Data using the Cryptographic Library on the Operating System.

F8 – Inter-Component Encryption

All data transmitted between TOE components is encrypted using the TLS protocol. The TOE calls the following encryption method:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA, which has the following attributes:
    - Key Exchange = RSA
    - Cipher algorithm =3DES_EDE_CBC
    - Hash algorithm = SHA

Application Note - This is carried out by calls to the Microsoft Cryptographic Service Providers (CSPs) and associated crypto algorithms associated with Windows 2003 CryptoAPI and Windows XP Professional Crypto API to encrypt/decrypt communication between TOE components. The cipher algorithm 3DES_EDE_CBC performs encryption of traffic between TOE components. The cipher algorithm 3DES_EDE_CBC specifies TripleDES in Encrypt-Decrypt-Encrypt mode with Cipher-Block Chaining. The size of the TripleDES key is 192 bits.

Further details can be found at http://www.ietf.org/rfc/rfc2246.txt.

F9– Domain re-authentication

It shall be possible for an administrator to configure the TOE such that Domain Re-Authentication will be invoked for specified controlled applications and after a set time period has elapsed.

Application Note – The Administrator can configure the TOE so that a user will be forced to perform a Domain Reauthentication either on the basis of certain critical applications or on the basis of a configurable time period having elapsed.

In the domain, a user will be configured with either a password or a certificate-based smartcard. If a user has a password then Domain Reauthentication is via the normal Windows Password authentication mechanism. If a user has been provided with a smartcard then Domain Reauthentication will be via the Windows smartcard authentication mechanism.

Password Manager provides support for Certificate-based smartcard solutions which provide added security when authenticating to the domain. The TOE supports PC/SC-based cryptographic smart cards which include support for digital signatures and encryption and require two factor authentication (the card and a pin number). Furthermore Cryptographic cards are designed to allow storage of private keys and also perform the actual cryptographic functions on the card itself, meaning that the private keys never leave the smartcard.

F10– Audit Generation

The TOE shall be able to generate an audit record (containing date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event) of the following audit events:

- Start-up and shutdown of the audit function;
- All successful and unsuccessful attempts by the TOE to submit secondary credentials to a controlled application;
- All changes to users' application passwords by the TOE in response to a password change request from a controlled application.

Application Note – The TOE generates a number of audit records which are then passed to the Window's Event Viewer for consideration by the Administrator.

F11– Residual Information Protection

The memory on the Agent machine holding cryptographic key material and application passwords will be zeroized before being made available to other processes.

6.2 Assurance Measures

Deliverables will be produced to comply with the Common Criteria security assurance requirements for EAL2, with the addition of ALC_FLR.2 (Flaw Reporting Procedures).

7 Protection Profiles Claims

There are no Protection Profile Claims.

8 Rationale

8.1 Introduction

This section identifies the rationale for the adequacy of the security functional requirements and the security assurance requirements in addressing the threats and meeting the objectives of the TOE.

8.2 Security Objectives for the TOE and Environment Rationale

The following table demonstrates how the objectives of the TOE and the TOE environment counter the threats identified in Section 3.2.1.

Note that all assumptions are axiomatic and hence not shown in this table. It would be possible to restate each one as an objective for the environment, and provide a one to one mapping for these, but this step has been omitted for clarity.

Threats / **Objectives**	T.USER	T.STRENGTH	T.ATTACK	T.ACCESS	T.WALKAWAY	T.PHISHING	T.MOD_HW	T.MOD_STORE	T.AUDIT_REVIEW	OSP.CRYPTO
OT.CONF	✓		✓	✓						
OT.INTEG			✓	✓		✓				
OT.APPLICATION	X		✓	✓						
OT.STRENGTH		✓	✓	✓						
OT.RE-AUTHN			✓	✓	✓					
OT.TIMEOUT			✓	✓	✓					
OT.PASSWORD	✓		✓	✓						
OT.PHISHING						✓				
OT.AUDIT			✓	✓						
OE.THIRD_PARTY			X	X						

Threats / Objectives	T.USER	T.STRENGTH	T.ATTACK	T.ACCESS	T.WALKAWAY	T.PHISHING	T.MOD_HW	T.MOD_STORE	T.AUDIT_REVIEW	OSP.CRYPTO
OE.SECURE_ENCRYPTION	X		X	X						✓
OE.SESSION_KEYS	X		X	X						
OE.AUDIT_REVIEW									✓	
OE.PHYSICAL							✓	✓		
OE.DESKTOP							✓			
OE.CERTIFICATES	X		X	X						

Table 8-1 Objectives Rationale

Key:

X Indirect contribution to meeting a threat

✔ Direct contribution to meeting a threat

As can be seen from the table above, all threats and organizational security policies are met by at least one objective of, either the TOE or environment, as applicable. The coverage of the threats countered by the TOE is discussed in the subsections below.

T.USER

OT.CONF and OT.PASSWORD ensure that the confidentiality of application passwords is not compromised, including not allowing the user of the credentials to see them.

In addition this threat is countered by the fact that the TOE is responsible for submitting credentials to applications (OT.APPLICATION) and the cryptography further protecting the credentials (OE.SECURE_ENCRYPTION, OE.SESSION_KEYS and OE.CERTIFICATES).

T.STRENGTH

OT.STRENGTH ensures that application passwords are generated and changed in order to ensure that they are not easily guessable.

T.ATTACK

An attacker is prevented from gaining unauthorised access to a controlled application by the TOE maintaining the confidentiality of application passwords. The Objective OT.CONF requires that the confidentiality of user application authentication credentials are maintained during processing and transmission between TOE components. This objective is supported by OT.PASSWORD which requires that the TOE will not expose application passwords to any user and OT.STRENGTH which imposes password policy restraints on the generation of a new password. In addition OT.APPLICATION ensures that the TOE provides the credentials to a controlled application.

An attacker is further prohibited from gaining access to a controlled application by OT.RE-AUTHN and OT.TIMEOUT which require a user to perform a domain reauthentication either for a specific application or after a certain time period has elapsed. By generating audit events (OT.AUDIT) the TOE also detects access to secondary credentials.

An attacker is prevented from gaining unauthorised access to TOE data by virtue of that fact that the integrity of Administrative Settings is provided by OT.INTEG.

This threat is also countered by securely configuring third party software (OE.THIRD_PARTY) and the cryptography within the product (OE.SECURE_ENCRYPTION, OE.SESSION_KEYS and OE.CERTIFICATES).

T.ACCESS

A user is prevented from gaining unauthorised access to a controlled application by the TOE maintaining the confidentiality of application passwords. The Objective OT.CONF requires that the confidentiality of user application authentication credentials are maintained during processing and transmission between TOE components. This objective is supported by OT.PASSWORD which requires that the TOE will not expose application passwords to any user and OT.STRENGTH which imposes password policy restraints on the generation of a new password. In addition OT.APPLICATION ensures that only the TOE can provide the credentials to an application.

A user is further prohibited from gaining access to another user's controlled applications by OT.RE-AUTHN and OT.TIMEOUT which require a user to perform a domain reauthentication either for a specific application or after a certain time period has elapsed. By generating audit events (OT.AUDIT) the TOE also detects access to secondary credentials.

A user is prevented from gaining unauthorised access to TOE data by virtue of that fact that the integrity of Administrative Settings is provided by OT.INTEG.

This threat is also countered by securely configuring third party software (OE.THIRD_PARTY) and the cryptography within the product

(OE.SECURE_ENCRYPTION, OE.SESSION_KEYS and OE.CERTIFICATES).

T.WALKAWAY

This threat is countered by OT.RE-AUTHN and OT.TIMEOUT. OT.RE-AUTHN requires the logged-in user to perform a domain re-authentication when particular controlled applications are opened, and OT.TIMEOUT can be used to require the logged-in user to perform a domain re-authentication after a certain time period has expired. Both of these objectives help to counter the threat that a user or attacker could use another user's existing session to access a controlled application.

T.PHISHING

This threat is countered by OT.PHISHING which ensures that the TOE only submits application credentials to the correct applications. This threat is also countered by OT.INTEG which ensures that, by signing the Administrative Data, an attacker cannot change settings relating to a controlled application (such as the URL of the application).

T.MOD_HW

This threat is countered by OE.PHYSICAL and OE.DESKTOP which ensures that all machines running TOE components are physically protected.

T.MOD_STORE

This threat is countered by OE.PHYSICAL which ensures that the machine running the Central Store is protected.

T.AUDIT_REVIEW

This threat is countered by OE.AUDIT_REVIEW which ensures that audit records are available to be examined by the authorised administrator.

OSP.CRYPTO

This organizational security policy is addressed by the TOE and environmental objectives that require FIPS140 approved cryptographic modules (OE.SECURE_ENCRYPTION).

8.3 Security Requirements Rationale

8.3.1 TOE security functional requirements are appropriate

The following table identifies which TOE SFRs satisfy the TOE Objectives defined in Section 4.1.1. The coverage of the objectives by the SFRs is discussed below.

Security Functional Requirements	FIA_SOS.2	FIA_UID.2(1)	FIA_UAU.2 (1)	FIA_UAU.6 (1)	FCS_COP.1 (1)	FCS_COP.1 (2)	FCS_COP.1 (3)	FCS_CKM.1 (1)	FCS_CKM.1 (2)	FCS_CKM.4 (1)	FCS_CKM.4 (2)	FMT_SMF.1	FPT_ITT.1 (1)	FPT_ITT.1 (2)	FPT_RVM.1	FDP_RIP.1	FAU_GEN.1
OT.CONF					✓		✓	✓		✓				✓		✓	
OT.INTEG						✓			✓		✓			✓		✓	
OT.APPLICATION	✓	✓	✓									✓			✓		
OT.STRENGTH	✓											✓					
OT.RE-AUTHN				✓								✓					
OT.TIMEOUT				✓								✓					
OT.PASSWORD	✓		✓		✓			✓		✓			✓		✓		
OT.PHISHING	✓														✓		
OT.AUDIT																	✓

Table 8-2 Mapping of TOE Objectives to TOE SFRs

These mappings are shown in the above table. Described below are the SFRs that satisfy specific objectives.

OT.CONF

This objective is provided by the encryption of secondary credentials and the TLS encryption between all TOE components (FCS_COP.1(1), FCS_COP.1(3), FCS_CKM.1(1), FCS_CKM.4(1) and FPT_ITT.1(2)). In addition the correct handling of cryptographic key material and application passwords within memory (FDP_RIP.1) helps to provide this objective[12].

OT.INTEG

This objective is provided by digitally signing the Administrative Data (FCS_COP.1(2), FCS_CKM.1(2), FCS_CKM.4(2) and FPT_ITT.1(2). In addition the correct handling of cryptographic key material and application passwords within memory (FDP_RIP.1) helps to provide this objective[12].

[12] FDP_RIP.1 is only applicable to the machine hosting the Agent. On the machines hosting the Service and Console, the functionality provided by FDP_RIP.1 is unnecessary due to the physical controls on these machines (see A.PHYSICAL).

OT.APPLICATION

This objective is provided by the TOE controlling the submission of secondary credentials to controlled applications (FIA_SOS.2, FIA_UID.2(1) and FIA_UAU.2 (1)) and also by FMT_SMF.1 which requires the Administrator to configure controlled applications and set a user's initial application password. In addition FPT_RVM.1 helps to provide this objective by ensuring that each attempt to open a controlled application is handled by the TOE.

OT.STRENGTH

This objective is provided by FIA_SOS.2 which ensures that all passwords generated by the TOE meet a defined password policy and also by FMT_SMF.1 which requires the Administrator to define a password policy of sufficient strength.

OT.RE-AUTHN

This objective is provided by FIA_UAU.6(1) which ensures that a domain reauthentication will be required for certain applications and also by FMT_SMF.1 which requires the Administrator to set this feature for certain 'critical' applications.

OT.TIMEOUT

This objective is provided by FIA_UAU.6(1) which ensures that a domain reauthentication will be required when a configurable time period has elapsed and also by FMT_SMF.1 which requires an Administrator to set this time period.

OT.PASSWORD

This objective is provided by the encryption of secondary credentials within the TOE (FCS_COP.1(1), FCS_CKM.1(1), FCS_CKM.4(1) and FPT_ITT.1(1). In addition this objective is provided by the TOE controlling the submission of application passwords to controlled applications (FIA_SOS.2 and FIA_UAU.2(1)). FPT_RVM.1 also helps to provide this objective by ensuring that each attempt to open a controlled application is handled by the TOE.

OT.PHISHING

This objective is provided by the TOE controlling the submission of secondary credentials to controlled applications (FIA_SOS.2). In addition FPT_RVM.1 helps to provide this objective by ensuring that each attempt to open a controlled application is handled by the TOE.

OT.AUDIT

This objective is provided by FAU_GEN.1 which ensures that all required audit events are generated by the TOE.

8.3.2 IT environment functional requirements are appropriate

The following table identifies which IT environment SFRs address the objectives for the IT environment defined in Section 4.2.1. The coverage of the objectives by the SFRs is discussed below. It should be noted that many of these objectives will be met through procedural and administrative measures, and as such there may be objectives that do not map to any of the included security functional requirements.

	OE.THIRD_ PARTY	OE.SECURE_ ENCRYPTION	OE.SESSION_ KEYS	OE.AUDIT_ REVIEW
FCS_CKM.1 (3)		✓		
FCS_CKM.1 (4)		✓		
FCS_CKM.1 (5)		✓	✓	
FCS_CKM.2 (1)		✓	✓	
FCS_CKM.4 (3)		✓		
FCS_CKM.4 (4)		✓		
FCS_CKM.4 (5)		✓	✓	
FCS_COP.1 (4)		✓		
FCS_COP.1 (5)		✓		
FCS_COP.1 (6)		✓		
FIA_UID.2 (2)	✓			
FIA_UAU.2 (2)	✓			

FIA_UAU.6 (2)	✓			
FIA_UID.2 (3)	✓			
FIA_UAU.2 (3)	✓			
FPT_SEP.1	✓			
FAU_SAR.1	✓			✓
FPT_STM.1	✓			

Table 8-3 Mapping of IT environment objectives to IT environment SFRs

OE.THIRD_PARTY

This objective relates to the need to configure the IT environment in a secure manner. This is essentially reliant upon sound administrative controls and is related to the environmental SFRs concerning Identification and Authentication, Domain Separation and Audit.

OE.SECURE_ENCRYPTION

This objective for FIPS140 approved encryption is addressed through all environmental cryptographic SFRs.

OE.SESSION_KEY

This objective is addressed through requirements that deal with all aspects of Key Management for the TLS encryption.

OE.AUDIT_REVIEW

This objective is addressed through requirements that deal with Audit Review.

8.3.3 Security Requirement dependencies are satisfied

TOE security functional requirements

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FIA_SOS.2	None	Satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FIA_UID.2(1)	None	Satisfied
FIA_UAU.2(1)	FIA_UID.1	Satisfied by FIA_UID.2 (1) (which is hierarchical to FIA_UID.1).
FIA_UAU.6(1)	None	Satisfied
FCS_COP.1 (1) and (2)	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (1) and (2) and FCS_CKM.4 (1) and (2). In the evaluated configuration the administrator has no control over the provision of the encryption and thus there are no security attributes relating to this SFR that can be configured. Therefore there is no requirement for FMT_MSA.2 in the evaluated configuration.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FCS_COP.1 (3)	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (5) and FCS_CKM.4 (5) in the IT Environment. See table below. In the evaluated configuration the administrator has no control over the provision of the encryption and thus there are no security attributes relating to this SFR that can be configured. Therefore there is no requirement for FMT_MSA.2 in the evaluated configuration.
FCS_CKM.1 (1) and (2)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_COP.1 (1) and (2) and FCS_CKM.4 (1) and (2). In the evaluated configuration the administrator has no control over the provision of the encryption and thus there are no security attributes relating to this SFR that can be configured. Therefore there is no requirement for FMT_MSA.2 in the evaluated configuration.

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FCS_CKM.4 (1) and (2)	FCS_ITC.1 or FCS_CKM.1, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (1) and (2). The argument for the exclusion of FMT_MSA.2 is provided in the row for FCS_CKM.1 above.
FMT_SMF.1	None	Satisfied
FPT_ITT.1 (1)	None	Satisfied
FPT_ITT.1 (2)	None	Satisfied
FPT_RVM.1	None	Satisfied
FDP_RIP.1	None	Satisfied
FAU_GEN.1	FPT_STM.1	Satisfied by FPT_STM.1 in the Environment.

Table 8-4 – Mapping of TOE SFR Dependencies

IT environment security functional requirements

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FCS_CKM.1 (3), (4) and (5)	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_COP.1 (4), (5), (6) and FCS_CKM.4 (3), (4), (5). In the evaluated configuration the ctyptographic settings are configured during the installation and configuration of the product. Once set there are no security attributes relating to this SFR that require configuration. Therefore there is no requirement for

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
		FMT_MSA.2 in the evaluated configuration.
FCS_CKM.2 (1)	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (5) and FCS_CKM.4 (5). The argument for the exclusion of FMT_MSA.2 is provided in the row for FCS_CKM.1 above.
FCS_CKM.4 (3), (4) and (5)	FCS_ITC.1 or FCS_CKM.1, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (3), (4) and (5). The argument for the exclusion of FMT_MSA.2 is provided in the row for FCS_CKM.1 above.
FCS_COP.1 (4), (5) and (6)	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_CKM.1 (3), (4), (5) and FCS_CKM.4 (3), (4), (5). The argument for the exclusion of FMT_MSA.2 is provided in the row for FCS_CKM.1 above.
FIA_UID.2 (2) and (3)	None	Satisfied
FIA_UAU.2 (2) and (3)	FIA_UID.1	Satisfied by FIA_UID.2 (2) and (3) which are hierarchical to FIA_UID.1.
FIA_UAU.6(2)	None	Satisfied
FPT_SEP.1	None	Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied by FAU_GEN.1

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FPT_STM.1	None	Satisfied

Table 8-5 Mapping of Environment SFR Dependencies

8.3.4 Security Requirements are mutually supportive

The only interactions between the security requirements specified for the TOE are those which are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.2. These interactions are specified in the CC Part 2, and are therefore mutually supportive

8.3.5 Security assurance requirements rationale

The assurance level EAL2 with the addition of ALC_FLR.2 was selected as providing a moderate level of independently assured security. This level of assurance should be sufficient to allow the TOE to be used to protect unclassified but sensitive information such as that found in government organizations. Such applications require evidence of third party functional and known vulnerability testing, good quality guidance documentation and a well specified external interface.

8.3.6 ST complies with the referenced PPs

This Security Target does not claim compliance with a Protection Profile.

8.4 IT security functions rationale

8.4.1 IT security functions are appropriate

The Table below provides a mapping of Section 6 IT functions to SFRs (Section 5.1).

IT Function	Security Functional Requirement(s)
F1	FMT_SMF.1(b), FPT_RVM.1
F2	FMT_SMF.1(c), FPT_RVM.1
F3	FIA_SOS.2, FMT_SMF.1(a), FPT_RVM.1
F4	FPT_ITT.1(1), FCS_COP.1 (1), FCS_COP.1 (3), FCS_CKM.1 (1), FCS_CKM.4 (1), FDP_RIP.1, FPT_RVM.1
F5	FIA_UID.2(1), FIA_UAU.2(1), FPT_RVM.1, FIA_SOS.2, FCS_COP.1 (2)

IT Function	Security Functional Requirement(s)
F6	FCS_COP.1 (1), FCS_CKM.1 (1), FCS_CKM.4 (1), FPT_RVM.1
F7	FCS_COP.1 (2), FCS_CKM.1 (2), FCS_CKM.4 (2), FPT_RVM.1
F8	FCS_COP.1 (3), FPT_ITT.1 (1), FPT_ITT.1 (2), FPT_RVM.1
F9	FIA_UAU.6(1), FMT_SMF.1(d), FMT_SMF.1(e), FPT_RVM.1
F10	FAU_GEN.1, FPT_RVM.1
F11	FDP_RIP.1, FPT_RVM.1

Table 8-6 Mapping of IT Functions to SFRs

As can be seen by the table above all Security Functional Requirements of the TOE are fully provided by the IT security functions specified in the TOE Summary Specification.

Also demonstrated in Table 8-6, all IT Security Functions identified for the TOE in the TOE Summary Specification are required to meet the TOE Security Functional Requirements.

Note that FPT_RVM.1 ensures that all and any security functionality of the TOE is invoked as required. As such, all Security Functions map to it.

F1 Application Definition

This function ensures that the administrator configures all controlled applications before they are accessed by a user. This provides FMT_SMF.1(b).

F2 Provisioning

This function provides FMT_SMF.1(c) and allows the administrator to manage a user's initial application credentials.

F3 Secondary Credential Generation

This function ensures that all Application Passwords generated by the TOE are generated in accordance with a defined password policy. This helps to provide FIA_SOS.2 and FMT_SMF.1(a).

F4 Secondary Credential Protection

This function relates to the encryption of Secondary Credentials and the TLS encryption between TOE components and provides the SFRs relating to these two

types of encryption. This function also helps to provide FDP_RIP.1.

F5 Application Management

This function ensures that upon all attempts to open a controlled application the TOE will submit the correct users' secondary credentials to the correct application. This helps to provide FIA_SOS.2, FIA_UID.2(1), FIA_UAU.2(1) and FCS_COP.1(2).

F6 Secondary Credential Encryption

This function relating to the 3DES encryption of secondary credentials provides the SFRs relating to this aspect of cryptography.

F7 Administrative Data Integrity

This function relating to digitally signing the Administrative Data provides the SFRs relating to this aspect of cryptography.

F8 Inter-Component Encryption

This function relating to the protection of TOE links by TLS encryption provides the SFRs relating to this aspect of cryptography.

F9 Domain Re-Authentication

This function relating to domain re-authentication provides part of the administrative SFR (FMT_SMF.1(d) and FMT_SMF.1(e)) in order to configure Domain Re-Authentication and also FIA_UAU.6(1) which provides Domain Re-Authentication.

F10 Audit Generation

This function provides the audit SFR FAU_GEN.1.

F11 Residual Information Protection

This function provides SFR FDP_RIP.1.

8.4.2 IT security functions are mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.4), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8-6.

8.4.3 Strength of Function claims are appropriate

The SoF claim made by the TOE is SOF-Medium, which is defined in the CC Part 1 as "adequate protection against straightforward or intentional breaches of security".

This claim relates to the TSF's ability to generate a user's application passwords in accordance with the password policy set by an administrator (FIA_SOS.2 and related

TSF F3). AVA_VLA.1, one of the assurance components from which the EAL2 assurance level is comprised, determines that "obvious vulnerabilities cannot be exploited in the intended environment of the TOE" (CC Part 3). Therefore, a SoF claim of SoF-Medium demonstrates that the function with an associated SoF would ensure that obvious vulnerabilities have been addressed.

Therefore, the claim of SoF-Medium TOE is viewed to be appropriate for this use.

8.4.4 Assurance measures satisfy assurance requirements

Table 8-7, below, provides a tracing of the Assurance Measures to the assurance requirements that they meet. From the table it can be seen that all assurance requirements trace to at least one assurance measure.

The assurance requirements identified in the table are those required to meet the CC assurance level EAL2, with the addition of ALC_FLR.2 (Flaw Reporting Procedures). As all assurance requirements are traced to at least one of the assurance measures and all of the assurance measures have been produced with EAL2 in mind, the assurance measures contain sufficient information to meet the assurance requirements of the TOE.

Assurance Measures (documentation)	Assurance Requirements Met by Assurance Measure	
Configuration Management Documentation	ACM_CAP.2	Configuration items
Delivery, Installation and generation Procedures	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation and start-up procedures
Functional Specification Documentation	ADV_FSP.1	Informal Functional Specification
High-Level Design Documentation	ADV_HLD.1	Descriptive high-level design
Flaw Remediation Documentation	ALC_FLR.2	Flaw reporting procedures
Correspondence Demonstration Document	ADV_RCR.1	Informal correspondence demonstration
Administrator Guidance Documentation	AGD_ADM.1	Administrator guidance

Assurance Measures (documentation)	Assurance Requirements Met by Assurance Measure	
User Guidance Documentation	AGD_USR.1	User guidance
Test Coverage Documentation	ATE_COV.1	Evidence of coverage
Test Plan and actual tests and Results	ATE_FUN.1	Functional testing
Independent Testing Resources	ATE_IND.2	Independent testing
Strength of Function Documentation	AVA_SOF.1	Strength of TOE security function evaluation
Vulnerability Assessment Analysis Documentation	AVA_VLA.1	Developer vulnerability analysis

Table 8-7 Mapping of Assurance Measures to Assurance Requirements

This page is intentionally blank