IBM Security Access Manager for Enterprise Single Sign-On Version 8.2 with IMS Server Interim Fix 4 and AccessAgent Fix Pack 22 Security Target

Version:	**1.19**
Status:	**Released**
Last Update:	**2014-03-05**

Trademarks

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- DB2®
- WebSphere®

The following terms are trademarks of Oracle Corporation:

- Java®
- Oracle®

The following terms are trademarks of Microsoft Corporation:

- Active Directory®
- SQL Server®
- Windows®
- Windows Server®

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.19	2014-03-05	Scott Chapman	Initial ST.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	IBM Security Access Manager for Enterprise Single Sign-On Version 8.2 with IMS Server Interim Fix 4 and AccessAgent Fix Pack 22 Security Target
Version:	1.19
Status:	Released
Date:	2014-03-05
Sponsor:	International Business Machines, Corporation
Developer:	International Business Machines, Corporation
Certification Body:	BSI
Certification ID:	BSI-DSZ-CC-0683
Keywords:	Security Access Manager, Enterprise Single Sign-On

1.2 TOE Identification

The TOE is IBM Security Access Manager for Enterprise Single Sign-On Version 8.2 with IMS Server Interim Fix 4 and AccessAgent Fix Pack 22.

1.3 TOE Type

The TOE type is an enterprise single sign-on product for Microsoft Windows-based systems and consists of software and guidance documentation.

1.4 TOE Overview

The Target of Evaluation (TOE) provides enterprises with single sign-on services, coupled with strong authentication and comprehensive auditing capabilities. The TOE keeps track of each user's application credentials (ID/password) in a credential Wallet, and helps users log onto the various applications. This is achieved through a client-side software "agent" called the AccessAgent that, in addition to automating application logons, provides application access audit logging. An important characteristic of the TOE is that this agent emulates the logon actions of the user using the application native logon interfaces – as such, it will work with applications as-is, without requiring any applications to be re-programmed or re-configured. The TOE includes a central server called the IMS (Integrated Management System) Server for storing user Wallets and for providing centralized management of users and policies.

1.4.1 Required non-TOE software

The Operational Environment for the TOE consists of the following required software products:

- Microsoft Windows XP and Windows 7 for the AccessAgents (32-bit and 64-bit Windows)
- Microsoft Windows Server 2008 (32-bit/64-bit) for the IMS Server
- Microsoft Active Directory (AD)
- WebSphere Application Server (WAS) 7.0 (32-bit only) required by the IMS Server
- One of the following SQL-based databases required by the IMS Server:
    - IBM DB2

  - Microsoft SQL Server
  - Oracle Database
- Java Runtime Environment (IBM Java 6 for WAS 7.0)
- IBM Global Security Kit (GSKit) version 8.0.14.21 required by the AccessAgent.

1.4.2 Intended method of use

The TOE is intended to be used in a distributed Microsoft Windows environment for the automatic authentication of users to applications. The TOE components use network security protocols (i.e., SSL, TLS) to protect network data from disclosure and modification when communicating between one another, so network eavesdropping attacks on TOE communication data is significantly diminished. (The network security protocols and all cryptographic operations used by the protocols including random number generation are provided by the Operational Environment.)

1.4.3 Major security features

The main security functions of the TOE are:

- Audit - Generation and review of audit records
- I&A - The identification and authentication of all users (regardless of their role)
- User data protection - Protection of user data stored within Wallets
- Security management - Role-based management of security behavior of the TOE

1.5 TOE Description

1.5.1 Introduction

The TOE is an enterprise single sign-on product for Microsoft Windows-based systems and consists of software and guidance documentation.

The TOE automatically enters user credentials into credential-requesting applications on behalf of the user once the user has successfully authenticated to the TOE.

For every user, the TOE maintains a set of application-to-user-credential mappings in a secure Wallet. Each Wallet is encrypted with a Common Symmetric Key (CSK) which is uniquely generated for each user. (The encryption operations and CSK key generation are performed by the Operational Environment at the request of the TOE. The TOE controls the flow of the cryptographic operations performed by the Operational Environment.) A more detailed description of Wallets and CSKs is provided in section 7.1.3.

The TOE contains several types of access policies that are used as configuration data by the TOE. These access policies are grouped into the following major categories:

- Machine policies - policies that affect a specific machine/computer (e.g., audit logging policies, desktop inactivity policies, some Wallet policies).
- System policies - policies applicable to all users and machines (e.g., auditing policies, password strength policies, some Wallet policies).
- User policies - policies that affect a specific user (e.g., Log on/Log off policies, some Wallet policies).

Of the policies referred to above, only the password strength policies are evaluated by this evaluation.

The TOE supports user role-based access control. Role-based access control is used to restrict user access to certain TOE operations. The TOE implements the following user roles which are referred to in the follow-on sections (for more detailed role descriptions, see section 7.1.4):

- Administrator
- Help desk
- User

1.5.2 Architecture

The TOE consists of multiple components executing in a distributed environment and communicating using the network. Figure 1 depicts the different components forming the product. Each of the green shaded components will be described in the subsequent sections. These green shaded components together form the TOE.

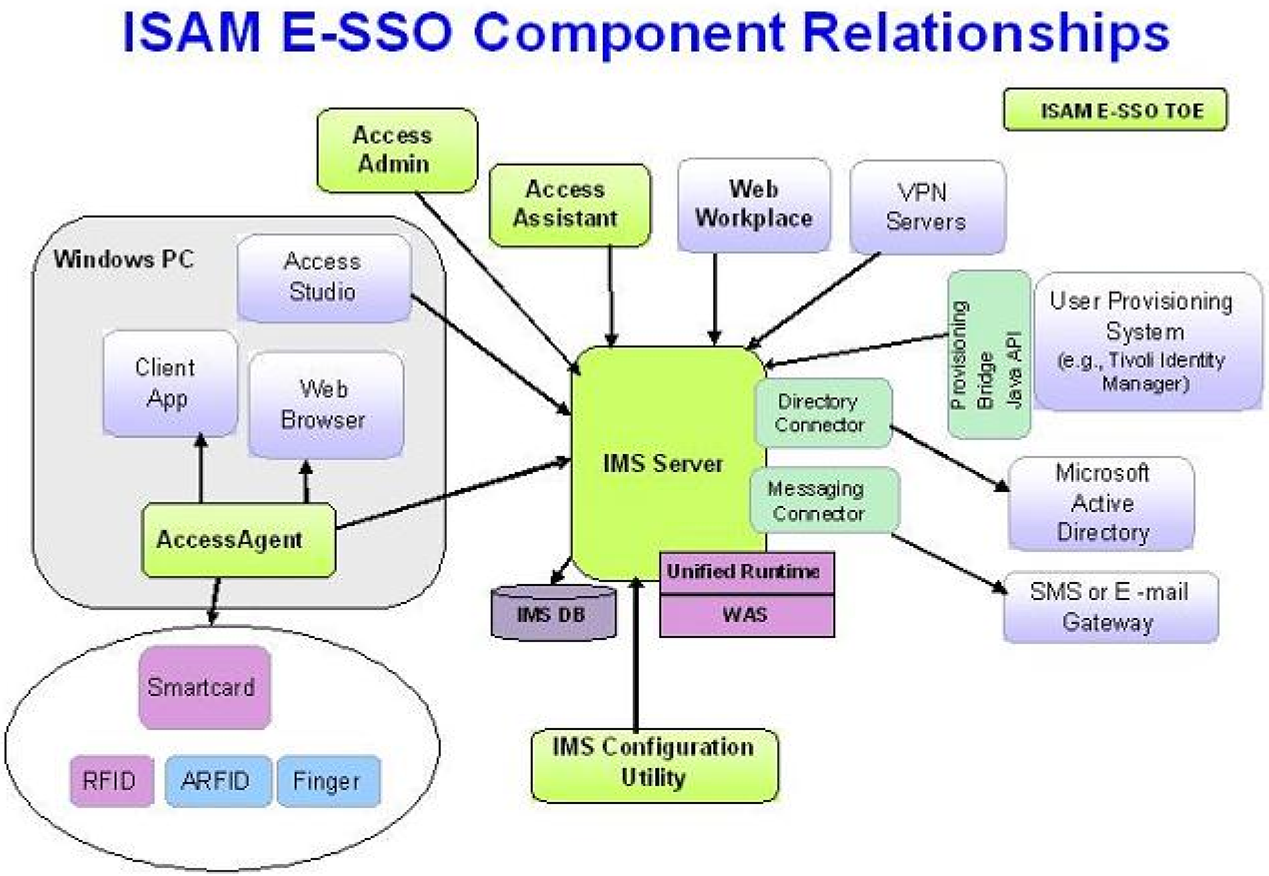

Figure 1: TOE Component Relationships

1.5.2.1 Communications

The relevant communication relationships for the TOE are shown in figure 2.

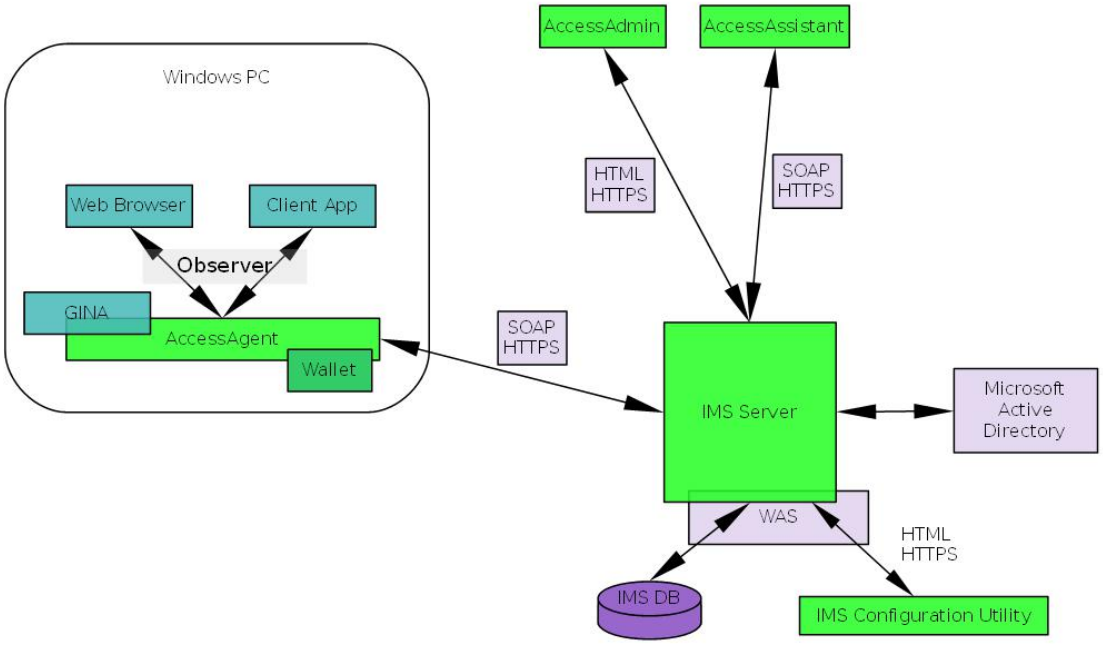

Figure 2: TOE Dataflow

1.5.2.2 The IMS Server

The IMS (Integrated Management System) Server serves as the central repository and management point for all system and user data consumed by the AccessAgents. The IMS Server performs the following functions:

- Serves as a central repository and distribution point for AccessProfiles and other system data.
- Serves as a central repository for all user data, including his credential Wallet and various authentication and access policies.
- Provides an internal SOAP API for AccessAgents, as well as AccessAssistant servers, to authenticate users, and to retrieve and synchronize system and user data.
- Provides Directory Connector SPI (not externalized) to enable integration with various user repositories. Refer to the IBM Security Access Manager for Enterprise Single Sign-On 8.2 RCS for the list of out of the box connectors that are provided.
- Provides a web-based UI (called "AccessAdmin") for managing users, machines and system policies, as well as to query audit logs.
- Creates a user's initial Wallet (including a CSK generated by the Operational Environment at the TOE's request) when a user account is created via the IMS Server.

Please note that the IMS DB (database) specifically marked in the illustration stores the data managed by the IMS Server, but the database system is not part of the TOE.

The TOE's IMS Server requires the use of the Microsoft Active Directory directory server in the evaluated configuration. The TOE can be configured to support password synchronization with Active Directory. When password synchronization with Active Directory is enabled, the Active Directory's password quality requirements are enforced by Active Directory, not the TOE. When password synchronization with Active Directory is disabled, the TOE's password quality requirements are enforced.

1.5.2.3 AccessAgent

The AccessAgent (AA) is the client software that is installed onto all Windows workstations at the TOE deployment site, and configured to connect to the designated IMS Server. The AccessAgent performs the following actions:

- Authenticates the end-user. Optionally, the AccessAgent protects access to the Windows desktop by replacing the native Microsoft Graphical Identification and Authentication (GINA) with the IBM Security Access Manager for Enterprise Single Sign-On GINA.
- Performs automated sign-on and sign-off to various applications. The AccessAgent has an Observer module that is hooked into various applications, and which consults the appropriate AccessProfile to perform the necessary logon/logoff and automation actions. The AccessAgent will log onto applications using the appropriate application credential retrieved from the user's credential Wallet.
- Tracks user application access activities and submits such audit events to the IMS Server.
- Synchronizes AccessProfiles, user's credential Wallet, and various Policy settings with the IMS Server.
- Provides a UI for end-users to manage the application credentials stored in their credential Wallet.
- Provides a UI for end-users to manage their own ISAM E-SSO Password.
- Creates a user's initial Wallet (including a CSK generated by the Operational Environment) when a user sign's up through the AccessAgent.

The AccessAgent can be deployed to Windows workstations with or without GINA replacement (i.e., in GINA mode or in GINA-less mode). In GINA mode, a user logs on to the IBM Security Access Manager for Enterprise Single Sign-On (ISAM E-SSO) GINA using his ISAM E-SSO username and password, whereupon the AccessAgent auto-logons to the Microsoft GINA with the user's Windows username and password. In GINA-less mode, a user will log on to Windows through the regular Microsoft GINA with his operating system username and password first, and the AccessAgent will then use the same credentials to log on the user to his cached Wallet and to the IMS Server.

The AccessAgent will contact the IMS Server upon start up, upon each user logon, as well as on periodic intervals, to synchronize system and user data changes with the server. However, the AccessAgent could cache data locally onto the hard disk. As such, it is able to perform most of its functions even if it is offline to the IMS Server at any point in time.

The AccessAgent relies on its Observer sub-module to perform its single sign-on and workflow automation features.

The Observer module is composed of an Observer Core module and a number of Observer agent instances that are hooked (through Windows APIs) into every Windows application (e.g. Lotus Notes, Outlook, Internet Explorer, etc) launched.

The behavior of the Observer agent within each specific Application is driven by a set of behavioral specifications called an AccessProfile. Each AccessProfile is an XML structure (based on a custom XML language) that provides a declarative set of preconditions (such as the signature of an application – e.g. name and version of the EXE file), a set of behavioral states (e.g. pre-logon, post-logon), and with each state, a set of triggers (e.g. when a specific screen is displayed) and actions (e.g. auto-fill username into a certain field) for the Observer agent to watch for and execute accordingly.

The Observer agents retrieve the required AccessProfiles as well as user credentials from the Observer Core module, which in turn communicates with the rest of the AccessAgent for data synchronization and session management services.

The AccessAgent controls access to a user's Wallet credentials so that only the application specified by the AccessProfile obtains the user's credentials specified for that application. This Wallet Access Control Policy is modeled in section 6.1.2.1 and is unique to the AccessAgent. The IMS Server and other TOE components provide only a supporting role for this policy.

The AccessAgent creates the initial Wallet for a new user when the user sign's up through the AccessAgent. The Wallet is used to hold the user's credentials for accessing other applications. The contents of the Wallet are encrypted by the Operational Environment at the request of the TOE using a 128 bit Common Symmetric Key (CSK). The generation of the CSK is also performed by the Operational Environment at the request of the TOE. The CSK is encrypted by the Operational Environment at the request of the TOE with the user's ISAM E-SSO Password and then stored with the Wallet in a file called a Cryptobox.

AccessAgent allows each user to change his own ISAM E-SSO Password. The TOE's password strength policies are enforced only when the AccessAgent is in GINA mode with Active Directory password synchronization disabled. When in GINA-less mode or when Active Directory password synchronization is enabled, the Active Directory's password strength policy is enforced by Active Directory, not the TOE.

1.5.2.4 AccessAdmin

The AccessAdmin application is the web-based management console used to administer the IMS Server, and to manage users (including modifying the role of each user) and policies.

The AccessAdmin application is installed with the IMS Server and allows the Administrator role to:

- Manage user authentication factors. (Only password authentication is allowed in the evaluated configuration.)
- Manage system, machine, and user policies.
- Manage machine and user groupings.
- Query audit logs; or generate out of the box audit reports

The AccessAdmin application is also used by the Help desk role to:

- Manage user authentication factors.
- Manage user policies.

1.5.2.5 AccessAssistant

The AccessAssistant is the web-based interface used to provide password self-help to end-users. In the evaluated configuration, it allows a user to:

- View and manage passwords for the various application accounts stored in the user's Wallet.

The AccessAssistant is implemented as a set of servlets that is by default deployed on the IMS Server.

1.5.2.6 IMS Configuration Utility

The IMS Configuration Utility is the web-based interface used to manage the configuration of the IMS Server. The IMS Configuration Utility application is installed with the IMS Server and allows the Administrator role to:

- Manage AccessProfiles
- Manage directory server configurations
- Manage database configurations

1.5.3 TOE boundaries

1.5.3.1 Physical

The TOE is comprised of the following components:

- IMS Server
- AccessAgent
- AccessAdmin
- AccessAssistant
- IMS Configuration Utility

The TOE is software only and is available in download format only from the IBM website. The TOE installation must include the Fix Packs specified in Table 1.

Component	Type	Name
AccessAgent	Fix Pack	8.2.0-ISS-SAMESSO-AA-FP0022
IMS Server	Interim Fix	8.2.0-ISS-SAMESSO-IMS-IF0004

Table 1: Required Fix Packs

The TOE guidance is available online through the Tivoli Software Information Center, except for the Common Criteria Guide which is available through the software download website. The relevant guidance documents for the secure operation of the TOE are:

- IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide
- IBM Security Access Manager for Enterprise Single Sign-On User Guide
- IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide
- IBM Security Access Manager for Enterprise Single Sign-On Common Criteria Guide

Section 1.4.1 lists the Operational Environment software products required by the TOE.

1.5.3.2 Logical

Due to the nature of the TOE storing, providing, and operating on user credentials for other applications, the TOE provides a number of security functions. Each security functional complex is identified and described below:

- Audit - The TOE has the ability to audit the user actions performed by all roles and to store the records in an audit trail using an external database. The Administrator role has the ability to review the audit trail using the AccessAdmin component or by using the provided database views.
- Identification and authentication - The TOE performs the identification and authentication of all users, regardless of their role, before it allows the user to perform any other actions.
- User credential protection - The TOE stores the user's credentials for third-party applications in the user's personal Wallet. A Wallet contains the user's arbitrary credentials which are treated as opaque user data by the TOE. By using encryption mechanisms in the Operational Environment, the TOE ensures the following:
  - Only owners have access to credential data.
  - The Administrator role can reset credential access data and restore use to a Wallet.
  - A third-party application is given only the credentials which are intended for this application and stored in the user's Wallet, preventing applications to "impersonate" as a different application to illicitly obtain credentials.
- Security Management - Role-based access control is used to protect access to operations in the AccessAdmin and AccessAssistant applications.

All cryptographic operations are performed by the Operational Environment.

1.5.3.3 Evaluated configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- The use of personal secrets must be disabled.
- Only the AccessAgent plugins provided with the TOE are allowed.
- Only the ISAM E-SSO Password authentication factor is allowed.
- Second factor authentication is disallowed.
- Self-service policies:
  - Self-service password reset must be disabled.
  - Self-service authorization code issuance must be disabled.
  - Self-service registration and bypass of 2nd factor must be disabled.
  - Self-service registering of additional secrets during sign-up must be disabled.
- The IMS Server's master secret must be protected to only allow the Administrator role access to it.
- One-Time Passwords (OTPs) must be disabled.
- Mobile ActiveCode (MAC) must be disabled.
- Roaming Desktops (i.e., the use of Microsoft Windows Terminal Server and Citrix Presentation Server) must be disabled.
- RADIUS authentication must be disabled.
- Windows Fast User Switching must be disabled on Windows 7 systems running AccessAgent.
- Private Desktop must be disabled on Windows XP systems running AccessAgent.

- Single sign-on to AccessAdmin when using Microsoft Internet Explorer must be disabled.
- The IMS Server/application must be the only application running in the WebSphere Application Server (WAS).
- The TOE's password synchronization option with Active Directory affects the security of the TOE. Specifically, enabling password synchronization with Active Directory will disable the TOE's ability to enforce password quality requirements.

1.5.4 Security policy model

The security policy for the TOE is defined by the security functional requirements in chapter 6. The following is a list of the subjects and objects participating in the policy.

Subjects:

- Users

Objects:

- Wallets
- Target applications

TSF data:

- AccessProfiles
- System policies, machine policies, and user policies
- User accounts, including the security attributes defined by FIA_ATD.1
- Audit records

User data:

- User credential data stored within Wallets.

2 CC Conformance Claim

This Security Target is CC Part 2 conformant and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL3, augmented by ALC_FLR.1.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 3 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are the following:

- The IMS Server stores all its data within a relational database. The IMS Server's database contains essentially these classes of data:
  - System data - AccessProfiles, system policies, machine policies, user policies, and other system configuration data
  - User data - credentials
  - Audit logs - user activities, administrative activities, SOAP event logs
- Additionally, the AccessAgent caches a subset of system and user data, so that it can continue to function even when disconnected with the IMS Server. The AccessAgent caches these data (in encrypted files) on workstations:
  - System/machine data - AccessProfiles, system policies, machine policies, and user policies
  - User data - application credentials
  - Audit logs - accessing of Wallet, using credentials out of the Wallet to provide to an application based on the AccessProfiles

The **threat agents** having an interest in manipulating the data model can be categorized as either:

- Unauthorized individuals ("attackers") which are unknown to the TOE and its runtime environment
- Authorized users of the TOE who try to manipulate data that they are not authorized to access

Threat agents originate from a well managed user community within an organizations internal network. Hence, only inadvertent or casual attempts to breach system security are expected from this community.

TOE administrators, including administrators of the TOE environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

3.1.1 Threats countered by the TOE

T.Manage

A threat agent gains access to the management facilities of the TOE allowing the modification of the security-relevant configuration of the TOE.

T.UserCredentials

A threat agent gains access to user credentials stored for a user by the TOE.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.Physical

It is assumed that the Operational Environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

3.2.1.2 Personnel

A.AuthUser

Authorized users are expected to act in a cooperating manner in a benign environment. Users are sufficiently trained and trusted to accomplish some task or group of tasks within the secure Operational Environment by exercising complete control over their user data.

A.Manage

The TOE security functionality as well as the TOE's underlying systems and of the systems in the TOE's Operational Environment that are involved in safeguarding TSF data or providing functionality that the TOE depends on is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

3.2.1.3 Logical

A.CryptoOps

The cryptographic operations performed by the Operational Environment are performed according to the specified algorithm standards and the random number generation provides sufficient randomness and entropy for key generation.

A.Remote

Threat agents are unable to violate the integrity, authenticity, and confidentiality of data exchanged between the components of the TOE distributed in the deployment infrastructure.

A.Repositories

Threat agents are unable to gain access to TSF data or user data stored in the Operational Environment, thus bypassing the TSF.

A.Runtime

The machines providing the runtime environment for the IMS Server are assumed to be used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying system and hardware. Especially, it is assumed that the underlying systems are configured in a way that prevents unauthorized access to security functions provided by or protected by the runtime environment either locally or via any network based connections.

A.System

Threat agents are unable to circumvent the TSF by penetrating or manipulating the runtime environment of the TOE and gain access to TSF or user data.

3.3 Organizational Security Policies

P.Accountability

Administrators and users are to be held accountable for security-relevant actions with the TOE.

P.PasswordQuality

The quality of the ISAM E-SSO Password protecting the Common Symmetric Key (CSK) must possess the strength to prevent credential guessing from threat agents.

P.User

Any user is trusted to perform the actions for which they have been authorized to perform. Authorized users possess the necessary authorization to perform at least one operation on the information managed by the TOE.

4 Security Objectives

4.1 Objectives for the TOE

O.AccessProfiles

The TOE must only releases a subset of the credential information stored in a user's Wallet to the target application the user intends to identify and authenticate to based on AccessProfiles.

O.Audit

The TOE shall offer an audit mechanism that can be used to hold users of each role accountable for security-relevant actions performed with the TSF. Security-relevant actions audited by the audit mechanism shall include password changes and the accessing of Wallets. Each audit record generated by the audit mechanism shall contain the time and date that the event occurred. The TOE shall provide a mechanism for authorized users to review the generated audit records.

O.Authentication

The TOE must ensure that only authorized users gain access to the TOE and its resources.

O.Manage

The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.

O.Role

The TOE must assign a role to each user after successful identification and authentication to the management facility. This role limits the management actions the user is allowed to perform.

O.PasswordQuality

When in GINA mode with Active Directory password synchronization disabled, the TOE must ensure that the quality of the ISAM E-SSO Password protecting the Common Symmetric Key (CSK) must possess the strength to prevent credential guessing from threat agents.

O.WalletAccess

The TOE must ensure that users can only access the contents of the Wallet assigned to them.

4.2 Objectives for the Operational Environment

OE.CryptoOps

The cryptographic operations performed by the Operational Environment shall perform according to the specified algorithm standards and the random number generation shall provide sufficient randomness and entropy for key generation.

OE.InfoProtect

Those responsible for the TOE must be competent individuals, not careless, willfully negligent, or hostile. They must follow and abide by the instructions provided by the guidance documentation. They must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

- All network communication channels and peripheral link must be approved for the transmittal of the most sensitive data held by the system. Such links are assumed to be adequately protected against threats to the authenticity, confidentiality and integrity of the data transmitted.
- All repositories holding TSF data and user data stored in the Operational Environment are access protected to restrict access to the TSF only.

OE.PasswordQuality

When either in GINA mode with Active Directory password synchronization enabled or when in GINA-less mode, the runtime environment must ensure that the quality of the ISAM E-SSO Password protecting the Common Symmetric Key (CSK) must possess the strength to prevent credential guessing from threat agents.

OE.Physical

Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives. The protection must commensurate with the value of the IT assets protected by the TOE.

OE.Runtime

The runtime environment used for all components of the TOE must be properly administered and protected from interference by unauthorized entities. This includes the requirement that the system(s) hosting components of the IMS Server are restricted to be used for this purpose only.

OE.TimeSource

The runtime environment shall provide a reliable time source for the TOE's use.

OE.Users

The TOE users shall act in a cooperating manner in a benign environment. The TOE users shall be trained and trusted to accomplish some task or group of tasks within the secure Operational Environment by exercising complete control over their user data.

4.3 Security Objectives Rationale

4.3.1 Security objectives coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.AccessProfiles	T.UserCredentials
O.Audit	P.Accountability
O.Authentication	T.Manage
O.Manage	T.Manage
O.Role	T.Manage P.User
O.PasswordQuality	P.PasswordQuality
O.WalletAccess	T.UserCredentials

Table 2: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.CryptoOps	A.CryptoOps
OE.InfoProtect	A.Manage A.Remote A.Repositories
OE.PasswordQuality	P.PasswordQuality
OE.Physical	A.Physical
OE.Runtime	A.Runtime A.System
OE.TimeSource	P.Accountability
OE.Users	A.AuthUser

Table 3: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Security objectives sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.Manage	The threat of unauthorized access to the management facilities of the TOE is diminished by the objective O.Manage which specifies that specific management facilities exist. In addition, a role mechanism is enforced for users with O.Role which supports the protection of the management facilities by limiting management capabilities of users to their role. For enforcing the role-based management mechanism, the TOE provides an identification and authentication mechanism for users with O.Authentication to allow the TOE to establish the user identity and the associated role for that user.
T.UserCredentials	The threat of unauthorized access to the credential data stored for a user by the TOE is diminished by the objective O.AccessProfiles which ensures that the TOE releases only the credentials required for a target application to the target application based on the AccessProfiles. An AccessProfile restricts other credentials in the Wallet from being decrypted by the Operational Environment and passed to a target application by mapping Wallet credentials to target applications. In addition, AccessProfiles provide methods to identify applications in order to prevent a threat agent from using a spoof or rogue application to obtain a user's credentials. In addition, the TOE implements per-user Wallets which the user must access using his ISAM E-SSO Password as specified with O.WalletAccess, ensuring that only the owner of a Wallet can access the user's Wallet holding the user's credentials.

Table 4: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.Physical	The assumption on physical protection of the TOE is achieved by the environmental objective OE.Physical to provide such protection.
A.AuthUser	The assumption that authorized users are cooperative, trained, and trusted is covered by the environmental objective OE.Users which requires that the TOE users shall act in a cooperating manner in a benign environment and the TOE users shall be trained and trusted to accomplish some task or group of tasks within the secure Operational Environment by exercising complete control over their user data.

Assumption	Rationale for security objectives
A.Manage	The assumptions that the management of the TOE and the underlying environment is conducted by competent individuals who are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation are achieved by the environmental objective OE.InfoProtect to ensure these properties of administrators.
A.CryptoOps	The assumptions that the cryptographic operations performed by the Operational Environment are performed according to the specified algorithm standards and the random number generation provides sufficient randomness and entropy for key generation are achieved by the environmental objective OE.CryptoOps which states that the cryptographic operations performed by the Operational Environment shall perform according to the specified algorithm standards and the random number generation shall provide sufficient randomness and entropy for key generation.
A.Remote	The assumption that threat agents are unable to compromise the exchange of data between the different distributed TOE components is achieved by the environmental objective OE.InfoProtect which guarantees that the environment protects these communication channels either by physical means (such as dedicated network links to which routing from outside networks is prohibited) or by logical means (such as the use of cryptographically secured network channels).
A.Repositories	The assumption that threat agents are unable to access the TOE repositories holding TSF data and user data and bypass the TSF is achieved by the environmental objective OE.InfoProtect which requires an appropriate access restriction of those repositories to the TSF.
A.Runtime	The assumption on exclusive TOE use of the underlying machines for the IMS Server and preventing unauthorized access to the TOE is achieved by the environmental objective OE.Runtime to implement corresponding measures for the server runtime environment.
A.System	The assumption that threat agents are unable to manipulate the runtime environment to circumvent the TSF is achieved by OE.Runtime which specifies that this runtime environment must be properly administered and protected from interference by unauthorized entities.

Table 5: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

OSP	Rationale for security objectives
P.Accountability	The policy to provide accountability for the action of TOE administrators and users is implemented by the objective O.Audit to provide an auditing mechanism and supported by the environmental objective OE.TimeSource to provide a reliable time source in the runtime environment.
P.PasswordQuality	The policy that the ISAM E-SSO Password must possess the strength to prevent credential guessing from threat agents is achieved by the objectives O.PasswordQuality and OE.PasswordQuality which require either the TOE or the runtime environment, respectively, to enforce the password strength depending on the TOE's configuration.
P.User	The policy that users are trusted to perform the actions for which they have been authorized to perform is achieved by the objective O.Role which ensures that the TOE assigns a role to every user identifying and authenticating with the TOE management facilities.

Table 6: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This Security Target does not extend the security components provided by the Common Criteria.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation	CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association	CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review	CC Part 2	No	Yes	Yes	No
	FAU_SAR.2 Restricted audit review	CC Part 2	No	No	No	No
	FAU_STG.1 Protected audit trail storage	CC Part 2	No	No	No	Yes
FDP - User data protection	FDP_ACC.2 Subset access control	CC Part 2	No	No	Yes	No
	FDP_ACF.1 Security attribute based access control	CC Part 2	No	No	Yes	No
FIA - Identification and authentication	FIA_ATD.1 User attribute definition	CC Part 2	No	No	Yes	No
	FIA_SOS.1 Verification of secrets	CC Part 2	No	No	Yes	No
	FIA_UAU.2 User authentication before any action	CC Part 2	No	No	No	No
	FIA_UID.2 User identification before any action	CC Part 2	No	No	No	No
	FIA_USB.1 User-subject binding	CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MSA.1 Management of security attributes	CC Part 2	No	No	Yes	Yes
	FMT_MSA.3 Static attribute initialisation	CC Part 2	No	No	Yes	Yes
	FMT_MTD.1 Management of TSF data	CC Part 2	No	No	Yes	Yes
	FMT_SMF.1 Specification of management functions	CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles	CC Part 2	No	No	Yes	No

Table 7: Security functional requirements for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **the following auditable events:**

- **IMS Server: logins, password changes, role changes, policy changes (for machine, system and user policies);**
- **AccessAgent: accessing of the Wallet, using credentials out of the Wallet to provide to an application based on the AccessProfiles, password changes.**

Application note: *The requirement to log startup and shutdown of the audit functions is trivially satisfied as the audit system is running when the TOE runs and cannot be turned off.*

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 (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **no other information**.

6.1.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **users assigned to the Administrator role** with the capability to read **all audit data** from the audit records *generated by the following audit events:*

- *IMS Server: logins, policy changes (for system and user policies only);*
- *AccessAgent: accessing of the Wallet, using credentials out of the Wallet to provide to an application based on the AccessProfiles.*

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: *The functionality of FAU_SAR.1 is provided by AccessAdmin.*

6.1.1.4 Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

6.1.2 User data protection (FDP)

6.1.2.1 Subset access control (FDP_ACC.2)

Wallet Access Control Policy		
Type	**Short name**	**Definition**
Subjects	S_User	A TOE user.
Objects	O_TargetApp	A target application.
	O_Wallet	A user's Wallet.
Operations	Decrypt	Decrypt the user's Common Symmetric Key (CSK) and the user's target application credentials (using cryptographic operations supplied by the Operational Environment).
	Release	Release the user's target application credentials for the specified target application.
Security attributes of subjects	AS_Password	A user's ISAM E-SSO Password for decrypting the user's CSK.
Security attributes of objects	AO_AccessProfile	The AccessProfile for the target application.
	AO_CSK	The user's CSK.
Rules	R_DecryptCSK	If the user's CSK can be successfully decrypted by the Operational Environment using a key derived from the user's ISAM E-SSO Password, then the TOE provides the user access to the user's Wallet; otherwise, access to the user's Wallet is denied.
	R_ReleaseCreds	If the target application's AccessProfile key is found in the user's Wallet, the user's credentials for only the target application are decrypted by the Operational Environment using the user's CSK and released to the target application; otherwise, no credentials are released to the target application.

Table 8: Wallet Access Control Policy

FDP_ACC.2.1 The TSF shall enforce the **Wallet Access Control Policy in Table 8** on **subjects and objects as defined in Table 8** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: *An AccessProfile key is a key created from information specific to an interface (e.g., a program's pathname and filename) that is used to reference the user's credentials for that program in the user's Wallet.*

Application Note: *The Wallet Access Control Policy defined in FDP_ACC.2 is only enforced by the AccessAgent. (The IMS Server does not enforce this policy.)*

6.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **Wallet Access Control Policy in Table 8** to objects based on the following: **subjects, objects, and for each the security attributes as defined in Table 8**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules as defined in Table 8 performed in the following order:**

1. **R_DecryptCSK;**
2. **R_ReleaseCreds.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

6.1.3 Identification and authentication (FIA)

6.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **User identifier;**
- **Common Symmetric Key (CSK);**
- **Role.**

6.1.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following:**

- **For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000;**
- **For multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 100,000; and**
- **Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.**

Application Note: *The password strength policies are enforced by the TOE only when the TOE is in GINA mode with Active Directory password synchronization disabled. The password strength policies are not enforced when the TOE is in GINA-less mode.*

6.1.3.3 User authentication before any action (FIA_UAU.2)

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.

6.1.3.4 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.5 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **User identifier (which is associated with auditable events);**
- **Role.**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **The IMS Server and all associated management interfaces: After successful identification and authentication, the user identifier and the role associated with the new session are set based on the identifier and role specified for the user entry of the successfully authenticated user.**
- **AccessAgent: After successful identification and authentication, the user identifier associated with the new session is set based on the identifier specified for the user entry of the successfully authenticated user.**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

6.1.4 Security management (FMT)

6.1.4.1 Management of security attributes (FMT_MSA.1)

Wallet Access Control Policy management		
Operations	**Security attributes**	**Authorized users and roles**
Add, modify	AccessProfile	Administrator role
Modify	ISAM E-SSO Password	Users who know the current ISAM E-SSO Password for the user's CSK

Table 9: Wallet Access Control Policy management

FMT_MSA.1.1 The TSF shall enforce the **Wallet Access Control Policy in Table 8** to restrict the ability to **perform the operations as defined in Table 9 on** the security attributes **as defined in Table 9** to **the authorized users and roles as defined in Table 9**.

Application Note: *To add and modify AccessProfiles, the IMS Configuration Utility is used. To modify ISAM E-SSO Passwords, AccessAgent is used.*

6.1.4.2 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Wallet Access Control Policy in Table 8** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 Management of TSF data (FMT_MTD.1)

TSF data management		
Operations	**TSF data**	**Authorized roles**
Modify	Role user security attribute	Administrator
Modify	System policies and machine policies	Administrator
View	System policies and machine policies	Administrator and Help desk
Modify, view	User policies	Administrator and Help desk

Table 10: TSF data management

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations in Table 10 on** the **TSF data in Table 10** to **the authorized roles in Table 10**.

Application Note: *To perform the operations on the TSF data specified in Table 10, AccessAdmin is used.*

6.1.4.4 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Assign roles to users (see FMT_MTD.1);**
- **Manage machine, system, and user policies (see FMT_MTD.1);**
- **View audit logs (see FAU_SAR.1).**

6.1.4.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

- **Administrator;**
- **Help desk;**
- **User.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2 Security Functional Requirements Rationale

6.2.1 Security requirements coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_STG.1	O.Audit
FDP_ACC.2	O.AccessProfiles, O.WalletAccess
FDP_ACF.1	O.AccessProfiles, O.WalletAccess
FIA_ATD.1	O.Authentication
FIA_SOS.1	O.PasswordQuality
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Authentication
FIA_USB.1	O.Audit, O.Authentication
FMT_MSA.1	O.Manage
FMT_MSA.3	O.Manage
FMT_MTD.1	O.Manage
FMT_SMF.1	O.Manage
FMT_SMR.1	O.Role

Table 11: Mapping of security functional requirements to security objectives

6.2.2 Security requirements sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.AccessProfiles	The access control policy specified with FDP_ACC.2 and FDP_ACF.1 ensures that only the intended credentials are released to the target application.
O.Audit	The objective to provide means to audit security-relevant actions with the TSF is met by requirements for audit record generation (FAU_GEN.1) and association of audited events with the originating user ID (FAU_GEN.2). Administrators have the ability to review audit data (FAU_SAR.1). The audit data is stored in a protected environment (FAU_STG.1) and the TOE ensures that it can only be read by authorized users (FAU_SAR.2). Users are identified based on the established identity during user-subject-binding (FIA_USB.1). The TOE environment needs to provide the proper time for the generated audit records, see OE.TimeSource. Supportive management functions have been specified in FMT_SMF.1.
O.Authentication	Identification and authentication is a prerequisite for the management function and is defined with FIA_UAU.2 and FIA_UID.2. After the successful identification and authentication, the TOE performs a user-subject-binding as defined with FIA_USB.1. The security attributes maintained by the TOE and used for the user-subject-binding are listed in FIA_ATD.1.
O.Manage	The general management functions provided with the TOE are listed in FMT_SMF.1 and detailed in FMT_MTD.1. In addition, the management of user Wallets is defined with FMT_MSA.1 and FMT_MSA.3.
O.Role	The definition of roles known to the TSF is specified with FMT_SMR.1.
O.PasswordQuality	When in GINA mode with Active Directory password synchronization disabled, the TOE ensures that the quality of the ISAM E-SSO Password protecting the Common Symmetric Key (CSK), as specified by FIA_SOS.1, must possess the strength to prevent credential guessing from threat agents.
O.WalletAccess	The access control policy specified with FDP_ACC.2 and FDP_ACF.1 ensures that users can only access their Wallet.

Table 12: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	The TOE is application software and, therefore, cannot provide reliable time stamps. Reliable time stamps must be provided by the Operational Environment. See OE.TimeSource.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FIA_ATD.1	No dependencies.	
FIA_SOS.1	No dependencies.	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	No dependencies.	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Table 13: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] part 3, augmented by ALC_FLR.1.

The following table shows the Security assurance requirements, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.3 Functional specification with complete summary	CC Part 3	No	No	No	No
	ADV_TDS.2 Architectural design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.3 Authorisation controls	CC Part 3	No	No	No	No
	ALC_CMS.3 Implementation representation CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_DVS.1 Identification of security measures	CC Part 3	No	No	No	No
	ALC_FLR.1 Basic flaw remediation	CC Part 3	No	No	No	No
	ALC_LCD.1 Developer defined life-cycle model	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.2 Analysis of coverage	CC Part 3	No	No	No	No
	ATE_DPT.1 Testing: basic design	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 14: Security assurance requirements

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match a Basic attack potential commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.1 commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

The following section explains how the security functions are implemented. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Audit
- Identification and Authentication
- User Data Protection
- Security Management

Of the policies referred to in the sections below, only the password strength policies are evaluated by this evaluation.

7.1.1 Audit

Various components of the product generate audit events which are stored in the IMS Server database.

All user application access logs are collated into the IMS Server's audit log database. Each log record contains info related to time and location from which a user accesses a certain application. Using AccessAdmin, the Administrator role can generate reports to review the logs contained in the database. Several predefined audit reports come standard with the TOE. Only users with the Administrator role are allowed access to the audit records via the TOE, preventing both unauthorized access to and unauthorized deletion of the stored audit records.

The TOE provides audit records for the following types of events besides the start-up and shutdown of the audit functions:

- IMS Server:
  - logins
  - password changes
  - role changes
  - policy changes (for machine, system and user policies)
- AccessAgent:
  - accessing of the Wallet
  - using credentials out of the Wallet to provide to an application based on the AccessProfiles
  - password changes

The audit records include the date and time of the event, the type of event, the subject identity and the event outcome. The audit record time stamps are obtained from a reliable time source in the Operational Environment.

The Administrator role can view and search a subset of the audit records through the TOE using AccessAdmin. The subset that can be viewed and searched are:

- IMS Server:
  - logins
  - policy changes (for system and user policies only)

- AccessAgent:
  - accessing of the Wallet
  - using credentials out of the Wallet to provide to an application based on the AccessProfiles

This section maps to the following SFR(s):

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1
- FAU_SAR.2
- FAU_STG.1

7.1.2 Identification and authentication (I&A)

The TOE supports an identification mechanism and an authentication mechanism. This section describes the supported mechanism.

The TOE maintains its own user repository, and performs user authentication against various forms of authentication credentials stored in this repository (stored in the IMS Server database). The user's ISAM E-SSO Password is created when the account is first created (when the user first sign's up).

The user's Wallet, which contains his authentication data, is stored centrally in the IMS Server database. Additionally, the authentication data is cached onto the user's workstation disk whenever the user caches his Wallet to a machine. This allows the AccessAgent to be able to authenticate users even when the machine cannot connect to the IMS Server.

An enterprise can ensure that its users use strong passwords to log on to the TOE by enforcing ISAM E-SSO Password strength policies.

7.1.2.1 AccessAgent

AccessAgent is a Windows application. It authenticates users based on their user identifier and password. A unique-per-user, 128 bit Common Symmetric Key (CSK) is generated by the Operational Environment at the request the AccessAgent for the user when the user initially sign's up through the AccessAgent. This CSK is associated with the user's account and is maintained by the TOE in the Cryptobox that contains the user's Wallet. The TOE passes the user's password along with the user's encrypted Common Symmetric Key (CSK) from the Cryptobox to the cryptographic operations in the Operational Environment to obtain the user's CSK. The user is considered authenticated by the TOE if the user's CSK is successfully obtained. (Authentication with one-time passwords (OTP) is disabled in the evaluated configuration.)

If the AccessAgent has a network connection to the IMS Server, it will authenticate a user against the user's credentials stored in the IMS Server, by passing along the authentication credentials over HTTPS to the IMS Server. However, if the AccessAgent is offline to the IMS Server, it will then authenticate the user's presented credentials against cached authentication data stored on the disk in the user's Cryptobox.

For AccessAgents installed with the GINA option enabled (i.e., in GINA mode), a user will log on to the AccessAgent GINA first, whereupon the AccessAgent will auto-logon the user into Windows using the user's Windows account.

For AccessAgents installed with the GINA option disabled (i.e., in GINA-less mode), the user will log on to Windows manually first, and then the AccessAgent will auto-logon the user into his Wallet.

Authentication of users by the AccessAgent is carried out in accordance to Authentication Policies defined by the Administrator role at the IMS Server and sync-ed to various AccessAgents.

AccessAgent allows each user to change his own ISAM E-SSO Password. The TOE's password strength policies are enforced only when the AccessAgent is in GINA mode with Active Directory password synchronization disabled. When in GINA-less mode or when Active Directory password synchronization is enabled, the Active Directory's password strength policy is enforced by Active Directory, not the TOE.

This section and its subsections map to the following SFR(s):

- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1

7.1.2.2 AccessAssistant

Users perform form-based logon to AccessAssistant using their username and ISAM E-SSO Password. The AccessAssistant authenticates a user by making SOAP-based logon calls, with the user-provided credentials, to the IMS Server, where the credentials are verified against the authentication data stored in the IMS Server database.

This section and its subsections map to the following SFR(s):

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1

7.1.2.3 AccessAdmin

Only users who are assigned Administrator or Help desk roles can log on to AccessAdmin. Users authenticate to AccessAdmin using the following method:

- Form-based logon (over HTTPS) using a username and ISAM E-SSO Password.

The authentication and access control is implemented by the AccessAdmin/IMS application, which will lookup the user's authentication data as well as assigned roles stored in the IMS Server database.

This section and its subsections map to the following SFR(s):

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1

7.1.2.4 IMS Configuration Utility

The IMS Configuration Utility is a web-based utility for editing the IMS Server's configuration. It uses authentication and access control provided by the Operational Environment.

7.1.3 User data protection

The TOE supports a user data protection mechanism. This section describes the supported mechanism.

The TOE stores each user's credential data in a Wallet; one Wallet per-user. A Wallet provides confidentiality and integrity protection of the user credential data through the use of cryptographic operations. All cryptographic operations are performed by the Operational Environment.

When a user sign's up via the TOE, the TOE creates a Wallet for the user and has the Operational Environment generate a 128 bit cryptographic key called the Common Symmetric Key (CSK).

The CSK is unique for each user and is used for encrypting the user's credential data stored in the user's Wallet. The CSK, in turn, is encrypted with a key derived from the user's ISAM E-SSO Password using AES 128 bit Cipher Block Chaining (CBC) mode. To decrypt items in the user's Wallet, the user supplies a valid ISAM E-SSO Password. The TOE provides the user's ISAM E-SSO Password and the user's encrypted CSK as input to cryptographic operations in the Operational Environment to obtain the CSK. The TOE then passes this CSK and an encrypted Wallet Credential from the user's Wallet as input to cryptographic operations in the Operational Environment to obtain a decrypted Wallet credential. For a user to change/modify the password of a Wallet, the user must know the current password for the TOE initiated decryption operations to succeed and to obtain the CSK. The AccessAgent allows each user to change his own ISAM E-SSO Password.

Both the Wallet and the password-encrypted CSK are stored in a secure data file on the AccessAgent called a Cryptobox; one Cryptobox per-user. The information in the Cryptobox is sent to the IMS Server for storage.

Since the CSK is required to access the credentials in the user's Wallet and the CSK is encrypted with the user's ISAM E-SSO Password, the TOE does not store user ISAM E-SSO Paswords anywhere in the system. Instead, the TOE requires users to supply their ISAM E-SSO Passwords each time they log in.

The IMS Server stores only the encrypted forms of the user's credential data and CSK. By default, the access controls on the IMS Server database are configured such that only an IMS Server-specific database account, and the database administrators are allowed to access the data.

Each Cryptobox file and its containing folder are protected by Windows ACLs, so normal Windows users will not be able to read and/or copy the files.

The AccessAgent's Single Sign-On function uses AccessProfiles to determine how to identify the target requesting the credentials, which credentials in the user's Wallet match the target, and how to provide the user's credentials to the target. If the target is an application, the AccessProfile specifies the executable path and file name, and the TOE uses these values to create a key, called an AccessProfile key, which is used to access the credentials in the user's Wallet. If the target uses GUI widgets, the AccessProfile specifies the GUI widgets, and the TOE uses the GUI widget values to create a key which is used to access the credentials in the user's Wallet. In addition, AccessProfiles can optionally specify workflow automation for use where complicated workflow is required. AccessProfiles are created and modified outside of the TOE using AccessStudio which is part of the Operational Environment. The IMS Configuration Utility is used to add new AccessProfiles to the IMS Server and to modify existing AccessProfiles that are used by the IMS Server.

Only the AccessAgent enforces the Wallet Access Control Policy defined by FDP_ACC.2 and FDP_ACF.1. The IMS Server and other TOE components provide only a supporting role for this policy.

This section maps to the following SFR(s):

- FDP_ACC.2

- FDP_ACF.1
- FMT_MSA.1
- FMT_MSA.3

7.1.4 Security management

The TOE supports security function management mechanisms. This section describes the supported mechanisms.

Role-based access control is used to protect access to operations in the AccessAdmin and AccessAssistant applications.

Users are classified into three roles:

- Administrator
- Help desk
- User

The Administrator role is the most powerful of all the roles. The Help desk role is more powerful than the User role, but less powerful than the Administrator role. The User role is the least powerful of the roles and is intended for ordinary users.

A new user is granted the User role by default when they first sign-up.

The initial Administrator user account is created during the IMS Server's configuration, using the IMS Web Configurator. Subsequently, an Administrator user can promote (i.e., modify the role of) any user to Administrator or Help desk role through the AccessAdmin interface.

Only users with Administrator role will have full access to the AccessAdmin application. For example, only Administrative users can modify machine policies and system policies. They can also view machine policies and system policies, and view and modify user policies.

The Help desk role provides some of the capabilities of the Administrator role. The Help desk role can view and modify user policies and view system policies and machine policies.

The TOE roles are stored in the IMS Server DB tables and managed by the AccessAdmin/IMS application. Access control (based on these roles) to the IMS Server's various services is enforced by the IMS Server.

The TOE contains several types of access policies that are used as configuration data by the TOE. These access policies are grouped into the following major categories:

- Machine policies
- System policies
- User policies

Machine policies are policies that affect a specific machine or computer. Policies in this category include the audit logging policies, desktop inactivity policies, and some of the Wallet-related policies such as limiting the number of Wallets allowed on a machine and only allowing the Wallet to be used on the machine where it was created.

System policies are policies that are applicable to all users and machines. Policies in this category include auditing policies, password strength policies, and some of the Wallet-related policies.

User policies are policies that affect a specific user. Policies in this category include the Log on/Log off policies and some of the Wallet-related policies such as the option for displaying of application passwords in AccessAgent.

This section maps to the following SFR(s):

- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

AA
AccessAgent

AD
Active Directory

AES
Advanced Encryption Standard

API
Application Programming Interface

CBC
Cipher Block Chaining

CSK
Common Symmetric Key

E-SSO
Enterprise Single Sign-On

GINA
Graphical Identification and Authentication

GSKit
IBM Global Security Toolkit

GUI
Graphical User Interface

HTTPS
Hypertext Transfer Protocol Secure

IMS
Integrated Management System

ISAM
IBM Security Access Manager

LDAP
Lightweight Directory Access Protocol

MAC
Mobile ActiveCode

OTP
One-Time Password

RADIUS
Remote Authentication Dial In User Service

RFID
Radio Frequency Identification

SFP
Security Function Policy

SFR
Security Functional Requirement

SOAP
Originally defined as Simple Object Access Protocol

SPI
Service Provider Interface

SSL
Secure Sockets Layer

SSO
Single Sign-On

ST
Security Target

TCP/IP
Transmission Control Protocol / Internet Protocol

TLS
Transport Layer Security

TOE
Target of Evaluation

TSF
TOE Security Functionality

UI
User Interface

USB
Universal Serial Bus

WAS
WebSphere Application Server

XML
Extensible Markup Language

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

AccessAgent
Client software that captures the user's credentials and acts on the user's behalf for single sign-on and sign-off.

Authentication Factors
Different methods for authenticating to the product, such as USB keys, biometrics, proximity cards, and passwords. See section 1.5.3.3 for the authentication factors supported in the evaluated configuration.

GINA-less mode
Defines the mode where the IBM Security Access Manager for Enterprise Single Sign-On (ISAM E-SSO) GINA is not installed on the operating system.

GINA mode
Defines the mode where the IBM Security Access Manager for Enterprise Single Sign-On (ISAM E-SSO) GINA is installed and used by the operating system.

GUI Widget
See Target Widget.

IMS Server
Provides centralized management of all users and policies. All policies are defined centrally and enforced through AccessAgent. The IMS Server also provides comprehensive back-up of credentials, loss management, audit, and compliance reporting.

Target Widget
A GUI widget belonging to an application monitored by the AccessAgent. The widget is monitored by the TOE and filled in with information from the user's Wallet when applicable. For example, a monitored application maintains a GUI widget referenced with "password" used to provide a password to log into the application. The AccessAgent monitors the application for that "password" widget in particular. If this widget is displayed, the AccessAgent detects the widget and fills in the password information for the monitored application from the user's Wallet.

User
Humans or machines interacting with the TOE via the provided user and programmatic interfaces. The term user in this document includes administrators of the TOE unless a specific distinction is made in the text.

Wallet
A personal, encrypted repository of user credentials. The Wallet roams to the point of access and stores the user's personal identity profiles, including log-in credentials, certificates, encryption keys, and user policies.

8.3 References

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R3
Date July 2009
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf