Forefront Identity Manager (FIM) 2010

Security Target

Common Criteria: EAL4 augmented with ALC_FLR.3

Version 1.0

24-MAR-2012

Document history

Version	Date	Description
0.1	28-APR-11	Initial draft for review.
0.2	26-MAY-11	Update to address comments.
0.3	17-FEB-12	Updated to reflect EOR005.
0.4	18-MAR-12	Internal review changes.
0.5	22-MAR-12	Internal review changes.
0.6	27-MAR-12	Updated to reflect EOR010.

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 Background

Today's IT enterprise must deliver identity and access management that is efficient, cost effective, and secure. The complexity of managing and securing users, devices, and services is increasing. Whether due to regulatory mandate or business growth, identity management becomes more complex, and often does not deliver as much business benefit as it could.

Nearly all organizations must manage identities, credentials, and resources across multiple directory trees and application-specific identity sources. Inefficient Identity management proves to be costly and inefficient for organizations. Manual or semi-automated management of identity information is costly and error-prone, especially when custom solutions and scripts are included. When users cannot manage their own identity and access needs, they push those operations back to the help desk, application owners and other IT departments.

Ensuring that only authorized users can access business resources in an enterprise environment is complex and expensive, especially as organisations grow. Centralising and controlling user, group, policy and credential management helps to improve the level of protection of corporate assets.

Forefront Identity Manager (FIM) 2010 provides an enterprise solution for addressing these issues and effectively and efficiently managing identities, credentials, and identity-based access policies across heterogeneous environments. FIM 2010 provides IT professionals with administrative tools to provision and manage digital identity and also provide end-users with self-service password reset capability and embeds self-help tools in Office so users can manage aspects of identity and access.

The core security functionality associated with the evaluation of the FIM 2010 solution includes the following:

a) controlling requests for access to identity resources protected by FIM 2010;

b) synchronising identity between disparate and disconnected sources of identity information;

c) controlling access to the FIM Portal and associated identity management functions and providing users with the capability to manager their own credentials and delegated identity information; and

d) effectively managing users, groups and policies.

1.2 ST reference

ST Title	Microsoft Forefront Identity Manager (FIM) 2010 Security Target
ST Version/Date	0.6 (27-MAR-2012)
TOE Reference	Microsoft Forefront Identity Manager 2010, which includes the following: a) FIM 2010 Service (Build 4.0.3547.2) b) FIM 2010 Synchronization Service (Build 4.0.3547.2) c) FIM 2010 Portal (Build 4.0.3547.2) FIM 2010 hotfix KB_2028634 March 23, 2011 The TOE also includes a suite of Management Agents and FIM Add-ins that have been identified in Section 1.5.1. Note: The Certificate Management functionality of FIM is excluded from the TOE.
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1 (REV 3) July 2009, incorporating: a) Part One – Introduction and General Model, b) Part Two – Security Functional Components, and c) Part Three – Security Assurance Component.

1.3 Document organization

This document is organized into the following major sections:

a) Section 1 provides the introductory material for the ST and the TOE overview (ASE_INT).

b) Section 2 provides the conformance claims for the evaluation (ASE_CCL).

c) Section 3 provides the definition of the security problem addressed by the TOE (ASE_SPD).

d) Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ).

e) Section 5 contains the security functional requirements derived from the Common Criteria, Part 2 (ASE_REQ).

f) Section 6 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ).

g) Section 7 provides the TOE summary specification that demonstrates how the TOE implements the claimed security functions.

h) Annex A provides defined terms (ASE_REQ).

i) Annex B provides a suite of correspondence mappings and required rationale.

1.4 TOE overview

1.4.1 TOE type

The TOE is an enterprise identity management solution—a suite of server components that manage identities, credentials and identity-based access policies across heterogeneous environments. The TOE can be categorised as an ***access control devices and systems*** in accordance with the categories identified on the Common Criteria Portal that lists all certified products.

1.4.2 TOE usage and major security features

The TOE is an enterprise software solution for managing digital identities, associated attributes and credentials throughout their entire lifecycle. The TOE provides identity synchronization services, centralised user provisioning and policy management that works across heterogeneous systems.

The TOE is to be used by IT professionals through administrative tools to provision, manage and control digital identity. The TOE also provides end-users with self-service password reset capability and embeds self-help tools in Office so users can manage aspects of identity and access.

The core security functionality associated with the evaluation of FIM 2010 includes the following:

a) **Resource request access control.** Implementation of controlled requested access to information resources protected by the TOE.

b) **Identity synchronisation.** Central synchronisation of identity information across a range of external and specified identity sources.

c) **Authentication and self-service.** Providing authentication controlled access to the FIM Portal and providing the capability for users to self-manage their identity information and credentials.

d) **Policy, user and group management.** A range of management functions aimed at effectively managing the core security policies implemented by FIM 2010.

1.5 TOE description

1.5.1 Physical scope of the TOE

FIM 2010 has many different components and in many deployment scenarios these components are not located on the same computer. As depicted in Figure 1 below, there are four (4) main software components that comprise the TOE:

a) **FIM Clients.** The TOE provides a number of different client-side components called a FIM Add-in that can be used for supporting the password reset functions and also workflow activities. The Password Reset Add-in can be deployed and integrated with the Windows client operating system to modify the logon process to allow anonymous (unauthenticated) users to reset their password. The FIM Add-in for Outlook allows approval requests to be approved or rejected directly from Office Outlook experience.

b) **FIM Portal.** A web-based user interface designed to provide the administrator with the capability to perform user, group and policy management and general administrative operations. The FIM Password Reset Portal also provides general users with the interface for performing self-service functions including password reset and identity management.

c) **FIM Service.** A web service that provides the centralised request-based access control features to ensure that requested access to identity resources is controlled in a secure manner. This web service implements a request processing model that comprises three distinct workflow steps: authentication, authorization, and action. Workflows (each of which contains one or more activities) can be attached to each of these steps and run in the context of executing a single request for access to protected identity resources.

d) **FIM Synchronization Service.** A centralized service that stores and integrates information for organizations that have multiple sources of identity information. The FIM Synchronization Service provides a unified view of all connected identity sources that can relate to users, applications, and network resources. The service manages information by receiving identity information from the connected data sources via Managed Agents and storing the information in the connector space as connector space objects. The connector space objects are then mapped to entries in the metaverse, called metaverse objects.

The following components are considered outside the physical scope of the TOE, but are necessary software elements that support the TOE in delivering the security objectives:

a) **Microsoft SQL Server.** Both the FIM Service and FIM Synchronization Service store their data in independent SQL databases.

b) **Identity Stores.** Also known as connected data sources are the systems that FIM manages through MAs. FIM 2010 includes several default MAs to manage a number of identity systems.

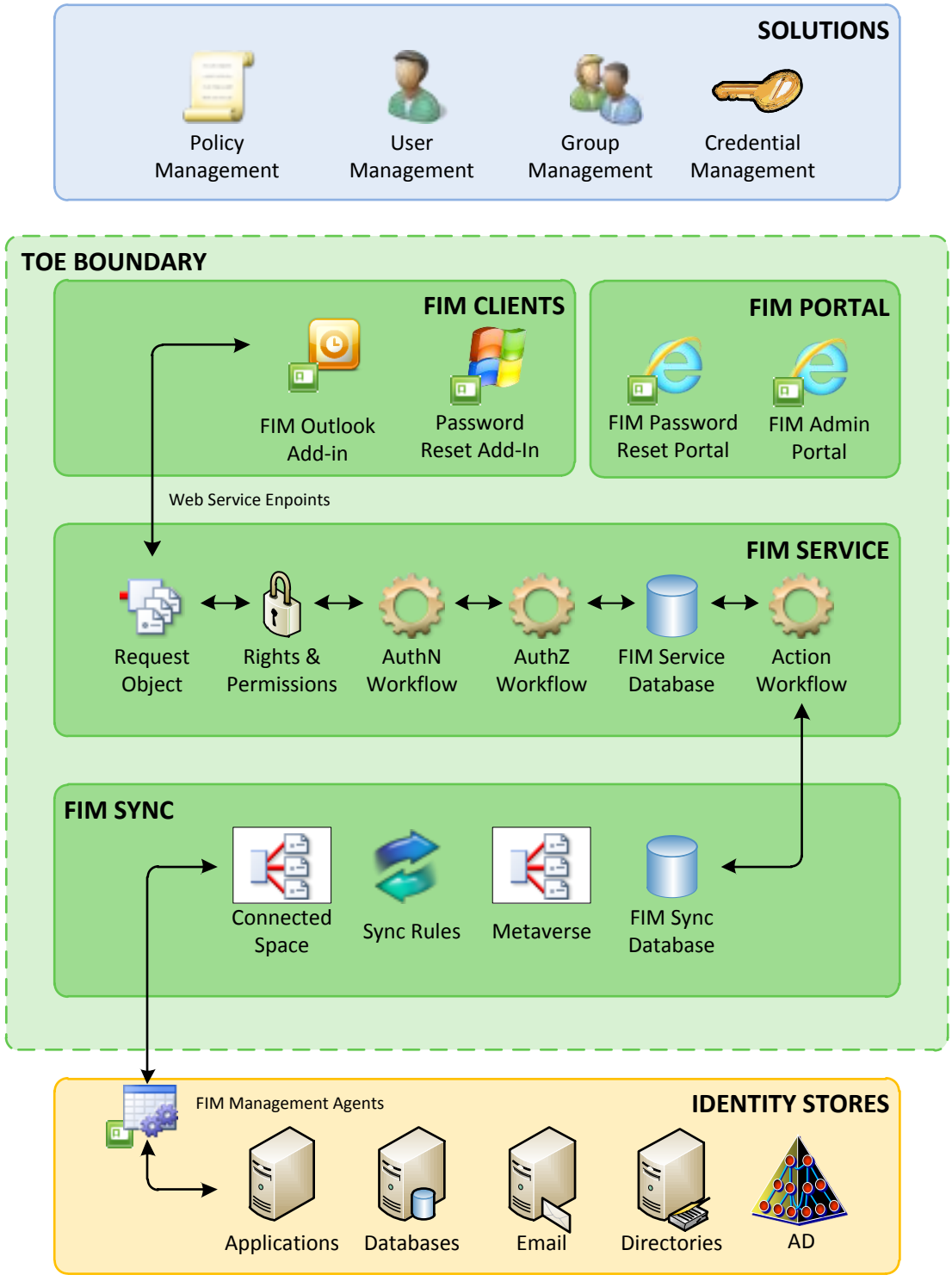

Figure 1 – TOE high-level architecture

1.5.2 Logical scope of the TOE

The logical scope of the TOE and the evaluation is centred on the core security functional policies and identity management activities as follows:

a) the request-based access control policy,

b) the synchronisation information flow policy,

c) identification and authentication associated with password reset and accessing the FIM Portal, and

d) general identity management activities that relate to policy, user and group management.

The evaluation or scope of the TOE does not include:

a) cryptographic protection of data in transit between the distributed components of the TOE,

b) protection of identity information in the various external identity stores, and

c) the implementation of custom add-ins or extensions.

d) **Management Agents.** Management agents link specific connected data sources to FIM 2010. A management agent is responsible for moving data from a connected data source to FIM. When data in FIM is modified, the management agent can also export the data out to the connected data source to keep the connected data source synchronized with the data in FIM.

e) **Certificate Management.** FIM provides credential management features to both Windows Server and 3rd party certification authorities (CAs) by acting as an administrative proxy. Once installed within an organization, all digital certificate and smartcard management functions pass through FIM.

1.5.3 Supporting hardware

The server or servers that host the FIM 2010 server components must meet the following minimum hardware requirements:

a) An x64-capable processor

b) 2 gigabytes (GB) of available hard disk space

c) 2 GB or more of RAM

d) A monitor with a resolution of 1024 × 768

e) A CD-ROM or DVD-ROM drive

The client computer that hosts the FIM 2010 client-side components must meet the following minimum hardware requirements:

a) 512 MB of RAM (1 GB recommended)

b) 500 MB of free hard disk space

c) A monitor that can display a resolution of 1024 × 768

1.5.4 Supporting software

Each server hosting the different FIM 2010 server-side components has a different software requirement. The following table provides the software requirements for each of the FIM 2010 server-side components. If all FIM 2010 server-side components are installed on one server, then all the software requirements for each of the FIM 2010 server-side components must be on that server.

The software requirements for the various FIM 2010 Management Agents are determined by the IT environment/software of the host identity store.

The following table provides the pre-requisite software required for each of the identified components of the TOE.

Component	Prerequisite software
FIM 2010 Synchronization Service software	• The 64-bit edition of the Windows Server 2008 or Windows Server 2008 R2 Standard or Enterprise operating systems • Windows Installer 4.5 • Microsoft SQL Server® 2008 64-bit Standard or Enterprise, Service Pack 1 (SP1) or later • Microsoft Visual Studio® 2008 • Windows PowerShell™ 1.0 or 2.0 • Microsoft .NET Framework 3.5 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2). • Exchange 2007 SP1 Management Console
FIM 2010 Service software requirements	• The 64-bit edition of Windows Server 2008 or Windows Server 2008 R2 Standard or Enterprise • Windows Installer 4.5 • 64-bit SQL Server 2008 Standard or Enterprise Editions, SP1 or later. • Windows PowerShell 1.0 or 2.0 • The .NET Framework 3.5 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2)
FIM 2010 Portal and Password Portal software requirements	• The 64-bit edition of Windows Server 2008 or Windows Server 2008 R2 Standard or Enterprise • The .NET Framework 3.5 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2) • Windows SharePoint Services 3.0 Language Pack

Component	Prerequisite software
FIM 2010 Management Agents	• As per the requirements of the host identity store.
FIM Add-ins and extensions components software requirements	• Windows XP Professional SP2 or later, 32-bit, Windows Vista Enterprise SP1 or later, 32-bit or 64-bit, or Windows 7 32-bit or 64-bit • Windows Installer 3.1 or later (only for Windows XP SP2) • Microsoft .NET Framework 3.5 SP1 • Microsoft Office Outlook® 2007 SP2 (Note: This software is required only if the FIM Office add-in is used).

2 Conformance Claim (ASE_CCL)

This ST is conformant to version **3.1 (Rev 3)** of the Common Criteria for Information Technology Security Evaluation.

The following specific conformance claims are made for this ST:

a) **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (Rev 3).

b) **Part 3 conformant, EAL4 augmented with ALC_FLR.3.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (Rev 3).

3 Security problem definition (ASE_SPD)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a set of ***threats*** that the TOE must mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) relevant ***organisational security policies*** that specify rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

In the context of this ST, the TOE has the following threat agents:

a) Individuals that have not been granted access to the TOE who attempt to gain access to information or functions provided by the TOE. This threat agent is considered an ***unauthorised individual***.

b) Individuals that are registered and have been explicitly granted access to the TOE who may attempt to access information or functions that they are not permitted to access. This threat agent is considered an ***unauthorised user***.

Identifier	Threat statement
T.REQUEST	An authenticated user may attempt to perform unauthorized actions on stored identity resources that may comprise the confidentiality and/or integrity of the stored identity information.
T.AUTH	An unauthorized individual may attempt to gain access to the TOE to perform either unauthorized actions on identity resources or perform unauthorized identity management activities that may compromise the confidentiality and/or integrity of the stored identity information.
T.EXPORT	Identity information may be exported outside the scope of control of the TOE in an insecure manner resulting in possible interception by an unauthorized individual and potential loss of integrity and confidentiality of the stored identity information.

Identifier	Threat statement
T.IMPORT	Identity information may be imported from outside the scope of control of the TOE in an insecure manner resulting in possible interception by an unauthorized individual and potential loss of integrity and confidentiality of the stored identity information.

3.3 Organisational security policies

In the context of this ST, the following organisational security policies (OSPs) are used to provide the basis for security objectives that are most often desired by acquirers and users of the TOE.

Identifier	OSP statement
P.SYNCH	Administrators must be capable of controlling the flow of identity information and ensure that authoritative information sources and attributes are maintained for both external and internal sources of identity information.
P.AUTHN	Administrators must be capable of implementing authentication workflow mechanisms to ensure that requesters for change or access to identity information can be effectively authenticated prior to committing changes to specific information resources.
P.AUTHZ	Administrators must be capable of implementing authorization workflow mechanisms to ensure that requesters for change or access to identity information can be effectively authorized prior to committing changes to specific information resources.
P.RESET	Users must be provided with the capability of registering to conduct self-service reset of authentication credentials in the case that a password has been forgotten or has expired.
P.AUTH_FAIL	Administrators must be capable of implementing a password reset policy that enables flexibility in selecting lockout methods and durations for failed password reset authentication attempts.
P.MANAGE	Administrators must be capable of performing the identity management related tasks including: user management, group management, policy management, and credential management.
P.ADMIN	Administrators must be capable of managing the various security functions and policies of the TOE.
P.DEFAULT	All identity resource objects that are created must have a default access rule of deny all.

3.4 Assumptions

The following assumptions provide the foundation for security objectives for the operational environment for the TOE.

Identifier	Assumption statement
A.FIREWALL	Any internet connection to a server role is assumed to be appropriately secured by a firewall.
A.INSTALL	It is assumed that the TOE will be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures. It is assumed that the administrator ensures that the machines the TOE is installed on support the secure operation of the TOE.
A.PLATFORM	It is assumed that the underlying server operating systems will provide the following: a) Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases only to the administrators authorized to perform these functions. b) Functionality for supporting and enforcing Identification and Authentication of users. It is assumed that the platform ensures the identification and authentication of users except for the case that they are performing the self-service function of the TOE. c) Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict the access to TSF data where necessary.
A.UNTRUSTED	It is assumed that no untrusted software is installed on the machines the TOE is installed on.
A.NO_EVIL	It is assumed that there will be one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain. It is also assumed that the administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
A.PROTECT	It is assumed that the TOE and its platform will be located within facilities providing controlled access to prevent unauthorized physical access.
A.PATH	It is assumed that the IT environment will provide a trusted communication path between itself and remote users for: a) use of the FIM clients transfer authentication data, b) access to the self-service portal by users, and c) access to the administrative interface by administrators.

4 Security objectives (ASE_OBJ)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.REQUEST	The TOE shall prevent an authenticated user from performing unauthorized actions on stored identity resources that may comprise the confidentiality and/or integrity of the stored identity information.
O.AUTH	The TOE shall prevent an unauthorized individual from gaining access to the TOE to performing either unauthorized actions on identity resources or performing unauthorized identity management activities that may compromise the confidentiality and/or integrity of the stored identity information.
O.EXPORT	The TOE shall prevent identity information from being exported outside the scope of control of the TOE in an insecure manner resulting in potential loss of integrity and confidentiality of the stored identity information.
O.IMPORT	The TOE shall prevent identity information from being imported from outside the scope of control of the TOE in an insecure manner resulting in potential loss of integrity and confidentiality of the stored identity information.
O.SYNCH	The TOE shall provide administrators with the ability to control the flow of identity information and ensure that authoritative information sources and attributes are maintained for both external and internal sources of identity information.
O.AUTHN	The TOE shall provide administrators with the capability to implement authentication workflow mechanisms to ensure that requesters for change or access to identity information can be effectively authenticated prior to committing changes to specific information resources.
O.AUTHZ	The TOE shall provide administrators with the capability to implement authorization workflow mechanisms to ensure that requesters for change or access to identity information can be effectively authorized prior to committing changes to specific information resources.

Identifier	Objective statements
O.RESET	The TOE shall provide users with the capability to register and perform self-service reset of authentication credentials in the case that a password has been forgotten or has expired.
O.AUTH_FAIL	The TOE shall provide administrators with the capability to implement a password reset policy that enables flexibility in selecting lockout methods and durations for failed password reset authentication attempts.
O.MANAGE	The TOE shall provide administrators with the capability to perform the following identity management related tasks: a) user management, b) group management, c) policy management, and d) credential management.
O.ADMIN	The TOE must provide administrators with the capability to manage the various security functions and policies of the TOE.
O.DEFAULT	The TOE must provide a default policy rules of deny all for all created identity resource objects.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.FIREWALL	The IT environment shall ensure that any internet connection to a server role is appropriately secured by a firewall.
OE.INSTALL	The operational environment shall ensure that the TOE is delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures. The operational environment shall enable the administrator to ensure that the machines the TOE is installed on support the secure operation of the TOE.

Identifier	Objective statements
OE.PLATFORM	The IT environment shall provide an underlying server platform that provides the following: d) Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases only to the administrators authorized to perform these functions. e) Functionality for supporting and enforcing Identification and Authentication of users. It is assumed that the platform ensures the identification and authentication of users except for the case that they are performing the self-service function of the TOE. f) Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict the access to TSF data where necessary.
OE.UNTRUSTED	The operational environment shall ensure that no untrusted software is installed on the machines the TOE is installed on.
OE.NO_EVIL	The operational environment shall provide one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain. The operational environment will ensure that the administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
OE.PROTECT	The operational environment will ensure that the TOE and its underlying platform are located within facilities providing controlled access to prevent unauthorized physical access.
OE.PATH	The TOE must provide all remote users with a trusted interface for authenticating to the TOE to ensure the confidentiality and integrity of user and TSF data.

5 Security functional requirements (ASE_REQ)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (Rev 3) of the CC, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the CC defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

The security functional requirements are expressed using the notation stated in Section 5.1 above and are identified in the table below.

Identifier	Title
User data protection (FDP)	
FDP_ACC.1	Subset access control (REQUEST)
FDP_ACF.1	Security attribute based access control (REQUEST)
FDP_IFC.1a	Subset information flow control (INBOUND)
FDP_IFF.1a	Simple security attributes (INBOUND)
FDP_IFC.1b	Subset information flow control (OUTBOUND)

Identifier	Title
FDP_IFF.1b	Simple security attributes (OUTBOUND)
FDP_ITC.1	Import of user data without security attributes
FDP_ETC.1	Export of user data without security attributes
FDP_ITT.1	Basic internal transfer protection
Identification and authentication (FIA)	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
Security management (FMT)	
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1a	Management of TSF data (USER)
FMT_MTD.1b	Management of TSF data (ADMINISTRATOR)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles

5.2 User data protection (FDP)

5.2.1 FDP_ACC.1 Subset access control (REQUEST)

Hierarchical to:	None
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [**REQUEST-SFP**] on [**a) Subjects:** **i. Request Object (operating on behalf of a Requester).** **b) Objects:** **i. Resource (Target).** **c) Operations:** **i. Create a resource.** **ii. Delete a resource.** **iii. Read and search a resource.** **iv. Modify a single-valued attribute of a resource.** **v. Add one or more values to a multi-valued attribute of a resource.** **vi. Remove one or more values of a multi-valued attributes of a resource**].
Notes:	This SFR describes one of the base access control policies that relate to the implementation of rules-based policies for FIM 2010. For users or requesters to access resources in the environment, the administrator will need to grant permission to perform operations on them. In logical policy statements, these are defined using access policies in the form of request-based policy statements. In a request-based policy statement, the condition consists of three components, the: a) Requester, b) target (or resource), and c) requested operation.

5.2.2 FDP_ACF.1 Security attribute based access control (REQUEST)

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1	The TSF shall enforce the [**REQUEST-SFP**] to objects based on the following:[**a) Request Object:** **i. Requester Unique Identifier (ObjectID).** **ii. Operation (Create, Delete, Enumerate, Get, Pull, Put, SystemEvent).** **iii. Target.** **iv. Request Endpoint (Alternate, Enumerate, Metadata Exchange, Password Reset, Resource, Resource Factory, Security Token Service).** **v. Security Token (where applicable).** **vi. Authorizations (where appropriate)** **b) Resource (Target):** **i. Object Unique Identifier (ObjectID)** **ii. Object Rules (DetectedRuleEntry and ExpectedRuleEntry)**].
FDP_ACF.1a.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) The Request Object must be matched to an MPR within the Object Rules that grants permission to the Resource (Target) for the requested operation.** **b) If any matched MPR includes an AuthenticationWF rule then the Requester must return a Security Token that confirms that the user has successfully completed each authentication process associated with the request.** **c) If any matched MPR included an AuthorizationWF rule then all authorization steps must be satisfied.** **d) If a related MPR provides access to the resource and all Authentication and Authorization Workflow conditions have been satisfied then the Requester is permitted to perform the requested Action on the Resource**].
FDP_ACF.1.3	The TSF shall explicitly authorise 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: [**a) If no MPR exists for the Target specified in the Request Object then the requested operation will be denied**].
Notes:	In the FIM 2010 model, granting permissions is only one aspect of a request-based policy statement. FIM access policies are flexible and customizable and the scope is not isolated to just granting permissions, it also permits the implementation of authentication and authorization workflow steps.

5.2.3 FDP_IFC.1a Subset information flow control (INBOUND)

Hierarchical to:	No other components
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1a.1	The TSF shall enforce the [**INBOUND-SFP**] on [**a) Subjects:** **i. Connector space objects (CSEntry).** **ii. Metaverse objects (MVEntry).** **b) Information:** **i. Identity information.** **c) Operations:** **i. Create connector space and metaverse objects.** **ii. Delete connector space and metaverse objects.** **iii. Process connector space and metaverse objects as a result of adding or removing links between objects.** **iv. Flow identity information from the connector space to the metaverse**].
Notes:	The FIM Synchronization Service is responsible for creating and distributing identity information using two (2) distinct steps: *inbound* and *outbound* synchronization. This SFR has been designed to model the *inbound* synchronization step of this process. Inbound synchronization creates and updates the integrated view of the identity information from the connected data sources. Inbound synchronization begins in the connector space and ends in the metaverse. Outbound synchronization distributes the integrated view of the identity information to all the connected data sources. Outbound synchronization begins in the metaverse and ends in the connector space.

5.2.4 FDP_IFF.1a Simple security attributes (INBOUND)

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1a.1	The TSF shall enforce the [**INBOUND-SFP**] based on the following types of subject and information security attributes: [**a) Subjects:** **i. ObjectID** **ii. Object Type (Metaverse or Connector)**

	b) Identity information **i. Source** **ii. Requested action**].
FDP_IFF.1a.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**a) Only those synchronization requests that pass the Connector Filter will be processed for synchronization (Connector Filter Rule).** **b) For all requests to delete an object the requested action must be permitted for the identity source if the change is to be synchronised to the metaverse (Object Deletion Rule).** **c) For all requests to join a connector object to a metaverse object the target object must exist in the metaverse otherwise the action will be rejected (Join Rule).** **d) For all requests to project the requesting connector object must have permission to create a metaverse object that can then be linked to the calling object (Projection Rule).** **e) For all synchronization requests, the Import Attribute Flow Rule must permit the synchronization of attributes from the source if identity attributes are to flow from the connector space object to the metaverse object (Import Attribute Flow Rule)**].
FDP_IFF.1a.3	The TSF shall enforce the [**none**].
FDP_IFF.1a.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1a.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Notes:	None.

5.2.5 FDP_IFC.1b Subset information flow control (OUTBOUND)

Hierarchical to:	No other components
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1b.1	The TSF shall enforce the [**OUTBOUND-SFP**] on [**a) Subjects:** **i. Connector space objects (CSEntry).** **ii. Metaverse objects (MVEntry).** **b) Information:** **i. Identity information.** **c) Operations:**

	i. **Create a new connector space object as a result of a change in the metaverse object.** ii. **Link a metaverse object to an existing connector space object.** iii. **Process connector space objects as a result of removing the link between the metaverse and connector space objects.** iv. **Flow identity information from the metaverse to the connector space**].
Notes:	The FIM Synchronization Service is responsible for creating and distributing identity information using two (2) distinct steps: *inbound* and *outbound* synchronization. This SFR has been designed to model the *outbound* synchronization step of this process. Outbound synchronization distributes the integrated view of the identity information to all the connected data sources. Outbound synchronization begins in the metaverse and ends in the connector space.

5.2.6 FDP_IFF.1b Simple security attributes (OUTBOUND)

Hierarchical to:	FDP_IFF.3 Limited illicit information flows
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1b.1	The TSF shall enforce the [**OUTBOUND-SFP**] based on the following types of subject and information security attributes: [**a) Subjects:** i. **ObjectID** ii. **Object Type (Metaverse or Connector)** **b) Identity information** i. **Source** ii. **Requested action**].
FDP_IFF.1b.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**a) For all provision requests the metaverse object must be permitted to create new connector space objects, or to connect or disconnect connector space objects as a result of a change to a metaverse object (Provisioning Rule).** **b) For all deprovision requests the metaverse object must be permitted to remove links between connector space objects as a result of a change to a metaverse object (Deprovisioning Rule).** **c) For all synchronization requests, the Export Attribute Flow Rule must permit the synchronization of attributes from the metaverse to the connector object if identity attributes are to flow to externally (Export Attribute Flow Rule)**

FDP_IFF.1b.3	The TSF shall enforce the [**none**].
FDP_IFF.1b.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1b.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Notes:	None.

5.2.7 FDP_ITC.1 Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [**INBOUND-SFP**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].
Notes:	This SFR provides assurance that the TOE user data, identity information, can be imported securely from external identity sources and both the FIM Service Database and the FIM Synchronization Service Database.

5.2.8 FDP_ETC.1 Export of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.1.1	The TSF shall enforce the [**OUTBOUND-SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes
Notes:	This SFR provides assurance that the TOE user data, identity information, can be transferred securely outside the scope of the TOE (from the Metaverse) to: Management Agents and then out to connected identity sources, and Microsoft SQL databases for both the FIM Service Database and the FIM Synchronization Service Database.

5.2.9 FDP_ITT.1 Basic internal transfer protection

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ITT.1.1	The TSF shall enforce the [**INBOUND-SFP and OUTBOUND-SFP**] to prevent the [***disclosure and modification***] of user data when it is transmitted between physically-separated parts of the TOE.
Notes:	This SFR provides assurance that identity information can move from the Management Agent through to the FIM Synchronization Service in a secure manner—free from the threat of disclosure and modification.

5.3 Identification and authentication (FIA)

5.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [***an administrator configurable positive integer within* [0 and 99]**] unsuccessful authentication attempts occur related to [**lockout**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**a) lockout the user from performing password resets for an administrator defined period of time (lockout duration), and** **b) permanently lock the account, requiring administrator intervention, when an administrator defined permanent lockout threshold has been met**].
Notes:	FIM implements a configurable password reset policy that provides the administrator with the capability of establishing a lockout policy that is suitable to the organisation and the operating environment.

5.3.2 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) user identifier,** **b) role(s),** **c) group(s),** **d) self-service status, and** **e) authentication data**].
Notes:	The TOE will maintain a range of information or attributes that relate to a specified user. Besides the normal identification and authentication attributes such as user identifier, role and group membership the TOE also maintains registration information and data relating to the status of a user's ability to perform self-service activities. In addition, the TOE will maintain authentication data including the challenge response data necessary for self-service activities.

5.3.3 FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow [**password reset**] on behalf of ~~the~~ **a self-service registered user** to be performed before the user is authenticated **using the common user authentication method**.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	The TOE provides the capability for a user that has registered with the self-service feature, to perform a password reset prior to being authenticated to the domain or the FIM Portal or any other method. The user must be registered and the policy enabled to support this feature of the TOE.

5.3.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide [**a) self-service password reset authentication challenge, and** **b) common authentication method**] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [following rules: **a) Only registered users are permitted to use the self-service password reset authentication challenge,** **b) All other TOE access must be through the common authentication method**].
Notes:	This SFR aims to demonstrate that the TOE provides two (2) distinct and separate methods for authenticating users. There is the general user authentication mechanism, which most commonly is the username/password associated with domain credentials and the implementation of a challenge response mechanism to provide users with the ability to reset their domain credentials in the case of forgotten or expired credentials. The term common has been used as this method is generally provided by the IT environment and could be a simple username/password combination or any other approved method that has been implemented within the specified IT environment.

5.3.5 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification.
Dependencies:	No dependencies.
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.
Notes:	None.

5.4 Security management (FMT)

5.4.1 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [**REQUEST-SFP, TRANSITION-SFP, PORTAL-SFP, INBOUND-SFP and OUTBOUND SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.
Notes:	In FIM, permissions for operations on all objects must be explicitly granted. Unless specifically granted by a management policy rule, all operations on resources are denied.

5.4.2 FMT_MTD.1a Management of TSF data (USER)

Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1a.1	The TSF shall restrict the ability to [***query, modify delete,*** **[create]**] the [**following TSF data:** **a) registration information,** **b) identity information that relates to the user, and** **c) authentication challenge questions**] to [**a user**].
Notes:	The user is capable of performing self-service registration and creating the authentication challenge information required for this step. In addition, the end-user has a certain amount of autonomy and control over their specific identity information.

5.4.3 FMT_MTD.1b Management of TSF data (ADMINISTRATOR)

Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1b.1	The TSF shall restrict the ability to [***query, modify delete,*** **[create]**] the [

	a) Request policy rules (MPRs), **b) Authentication workflow rules,** **c) Authorization workflow rules,** **d) Synchronization rules,** **e) Self-service policy, and** **f) Portal access policy**] to [**Administrator**].
Notes:	The administrator is responsible for managing the core TSF data elements that relate to establishing and managing security functional policies for the TOE.

5.4.4 FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) user management,** **b) group management (including security and distribution groups),** **c) self-service management (including profile and password-reset),** **d) request and policy management,** **e) synchronisation management, and** **f) portal configuration**].
Notes:	None.

5.4.5 FMT_SMR.1 Security roles

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [**a) user, and** **b) administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Notes:	The TOE permits the establishment of a range of groups and roles; however, as a general implementation the TOE establishes privileged users (administrators) and general users of the TOE.

6 Security assurance requirements (ASE_REQ)

This ST implements the Security Assurance Requirements (SARs) of the EAL4 package and augments this package with the inclusion of the ALC_FLR.3, systematic flaw remediation.

EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation and a description of the modular design of the TOE. The full implementation is also provided to the evaluator so that analysis can be conducted of an evaluator-selected subset, so that security behaviour can be understood and potential vulnerabilities identified.

The analysis is supported by independent testing of the TSF, which can be based on evidence of developer testing of the functions of the TOE. In addition, the evaluators will conduct a vulnerability analysis using all provided inputs and ensure that the TOE is resistant to penetration attackers with an ***enhanced-basic*** attack potential. EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

The selected set of SARs is appropriate due to the intended enterprise operating environment and customer base that this product is intended for. EAL4 provides evaluators with access to the implementation details for the TOE and enables deep analysis to identify potential vulnerabilities and exposures which is relevant and expected of an enterprise-grade software product.

EAL4 provides the right balance with understanding and documenting the modular structure of the TOE and the implementation detail, and providing sufficient assurance through independent functional and penetration testing. The following table highlights the assurance requirements of the EAL4 assurance package.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.4 Production support, acceptance procedures and automation

Assurance class	Assurance components
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

7 TOE summary specification

7.1 Overview

This chapter provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE implements the following security functions that suitably address the claimed set of requirements.

Security function	Description	Implemented SFRs
Resource request access control	Implementation of controlled requested access to information resources protected by the TOE.	FDP_ACC.1 FDP_ACF.1
Identity synchronisation	Central synchronisation of identity information across a range of external and specified identity sources.	FDP_IFC.1a FDP_IFF.1a FDP_IFC.1b FDP_IFF.1b FDP_ITC.1 FDP_ETC.1 FDP_ITT.1
Authentication and self-service	Providing the capability for users to self-manage their identity information and credentials.	FIA_AFL.1 FIA_ATD.1 FIA_UAU.1 FIA_UAU.5 FIA_UID.2
Policy, user and group management	A range of management functions aimed at effectively managing the core security policies implemented by FIM 2010.	FMT_MSA.3 FMT_MTD.1a FMT_MTD.1b FMT_SMF.1 FMT_SMR.1

7.2 Resource request access control

All users, groups, requests, workflows, and other resources used in FIM are stored as objects in the FIM Service database. These objects can be modified through Create, Read, Update, and Delete (CRUD) requests made to the FIM Service.

Web service requests are turned into Request objects in the FIM system. If a CRUD request on the object store passes the rights, authentication, and authorization checks, the CRUD operation will be run on the object store and the associated Request object will itself be committed to the object store. After this step, additional "Action" workflows (for example, notification activities) are run. These workflows can include actions performed by the synchronization engine, which manages synchronization of object changes with identity stores external to FIM.

Figure 2 below illustrates the request-based access control model that is a core security function of the TOE. As depicted, requests for access to identity resources are processed as follows:

a) **Request Object Creation.** The TOE creates a Request object in response to a call to one of the web service endpoints or because of a request initiated through the FIM Portal.

b) **MPR Evaluation.** The requester's rights to request the action are validated and the computation of the applicable workflows is performed. The request is checked against mappings to any MPR objects. To map to an MPR, all the applicable fields of the MPR for the requested operation need to match. This includes the requester, operation, target resource, and attributes. If all of these conditions including the attributes being affected are true for an incoming request, then the appropriate MPR is matched to the request. A request must map to at least one MPR that grants the permission as part of its definition. If this is true, the request passes through the permissions check stage of request processing. If this is not true, the request fails. The system also determines the set transitions that are part of the request and locates all related set transition-based MPRs.

c) **Authentication.** The TOE runs authentication workflows one at a time in a nondeterministic order to confirm the requester's identity.

d) **Authorization.** The TOE confirms the requester's permission to perform the requested operation on the resource specified in the request. All dependent authorization workflows are run in parallel, but a request is not committed to the FIM Object Store unless all of the workflows have been completed and all have succeeded.

e) **Processing.** The TOE performs the requested operation on the FIM Application Store.

f) **Action.**-The TOE executes any processes that are to occur because of the requested operation. All action workflows are run in parallel. Read operations do not have any workflows applied to their processing. This includes the configured workflows in the request-based MPR as well as the workflows in the set transition-based MPRs.

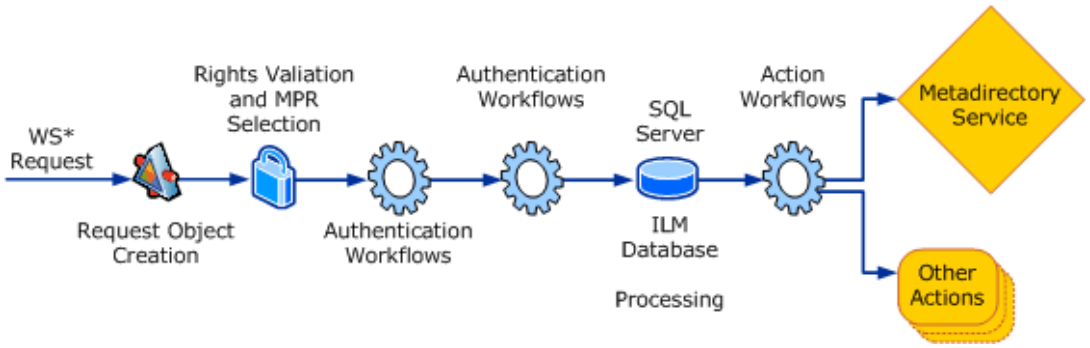

Figure 2 – Processing of requests

7.3 Identity synchronization

The FIM Synchronization Service provides the central capability for synchronizing identity data for the TOE. The goal of FIM Synchronization Service is to provide organizations with a unified view of all known identity information about users, applications, and network resources.

Figure 3 below shows how the identity data is organised and stored in the context of the FIM Synchronization Service.

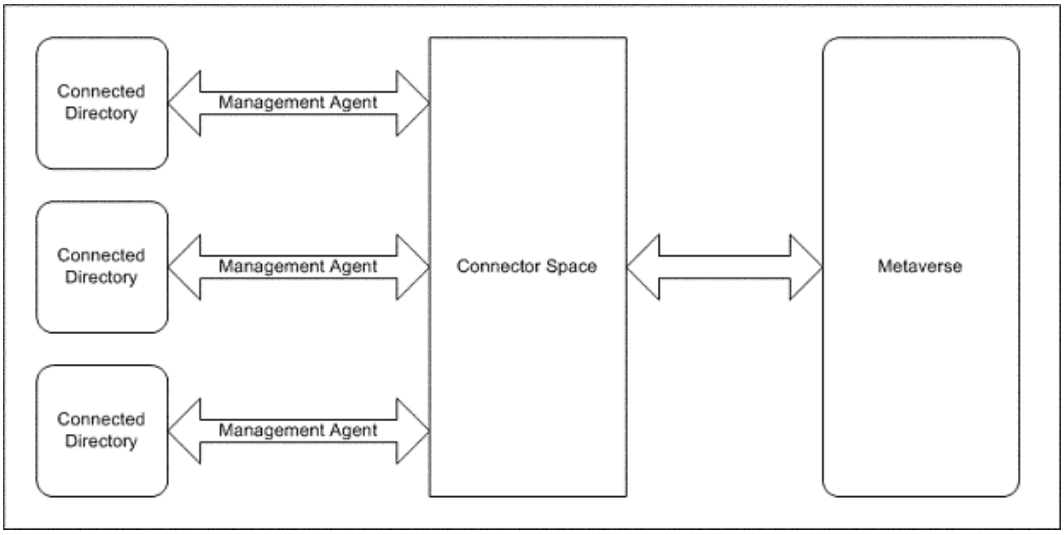

Figure 3 – Information flow and repositories for identity data

FIM Synchronization Service manages information by receiving identity information from the connected data sources and storing the information in the connector space as *connector space objects* or *CSEntry* objects. The *CSEntry* objects are then mapped to entries in the metaverse, called metaverse objects, or *MVEntry* objects. Using this process, you can map data from separate connected data sources to the same *MVEntry* object.

The information flow control policies relate to the implementation of identity synchronization services by the TOE. The FIM Synchronization Service processes identity information by creating an integrated view of the information in the connected data sources. This integrated view is referred to

as the metaverse. Data from this integrated view is then appropriately distributed so that all objects in the connected data sources contain this integrated view as appropriate.

Creating and distributing identity information in FIM Synchronization Service is known as the synchronization process. The synchronization process consists of the following two distinct steps (each has a separate information flow control policy):

a) **Inbound synchronization.** Creates and updates the integrated view of the identity information from the connected data sources. Inbound synchronization begins in the connector space and ends in the metaverse.

b) **Outbound synchronization.** Distributes the integrated view of the identity information to all the connected data sources. Outbound synchronization begins in the metaverse and ends in the connector space.

The synchronization process is started from a full or delta synchronization step in a run profile. The process begins with inbound synchronization to determine whether identity data must be processed from the connector space to the metaverse, and how it will be processed. In inbound synchronization, the synchronization process uses the synchronization rules to perform the following tasks between the connector space and metaverse:

a) Create or delete connector space and metaverse objects.

b) Process connector space and metaverse objects as a result of adding or removing links between objects.

c) Flow identity information from the connector space to the metaverse.

Only after inbound synchronization is completed can the outbound synchronization step begin. Outbound synchronization distributes the integrated view from the metaverse to the connector space. This view may be exported to the connected data source. Because an object in a connector space represents the identity information in a connected data source, this object contains only the attributes from that connected data source. FIM Synchronization Service distributes only the values for the object attributes in that connector space partition.

In outbound synchronization, the synchronization process uses the synchronization rules to perform the following tasks between the metaverse and connector space:

a) Create a new connector space object as a result of a change in the metaverse object.

b) Link a metaverse object to an existing connector space object.

c) Process connector space objects as a result of removing the link between the metaverse and connector space objects.

d) Flow identity information from the metaverse to the connector space.

7.4 Authentication and self-service

Components of password management

FIM provides the capability for users to register for self-service password reset. This allows users to reset their passwords by answering some or all of the questions answered during registration.

Password management in FIM 2010 consists of two components:

a) The FIM Password Reset Portal

b) The FIM Password Reset client, which is installed as part of the FIM Add-ins and Extensions.

Password Registration

To use password management, users must first register, which involves creating answers to a series of security questions. To reset their password, users will then be presented with these questions and they must provide the correct answers.

The password registration process involves these steps:

a) The user selects Register for password reset in the FIM Portal, which starts the password reset client.

b) The client displays a set of authentication challenge questions to the end user and gathers the end user response data, and then submits the response data to the FIM server.

c) The client returns a success or failure confirmation message to the user.

Password Reset

When a user has registered successfully, he or she can then use the Password Reset Portal to reset a forgotten password. The password reset process involves the following steps:

a) The user selects Reset in the Password Reset Portal or on the Windows logon screen, and the client initiates the request to reset the password.

b) The client displays the authentication challenge questions that the user configured during registration, and then it submits the user's response data to the FIM Server.

c) If a Lockout Gate activity has been configured by the administrator, a specified number of incorrect attempts may prevent the user from attempting the password reset for a specified period of time or necessitate calling the help desk.

d) Upon successful verification, the application displays the client user interface to create a new password and submits the user's response.

e) The application returns a success or failure confirmation to the user.

Verifying the challenge responses

When the user requests to reset their password, the Password Reset Portal page is displayed to the user, displaying the challenge questions previously configured in the Question and Answer gate, which the Password Reset Registration Web Application displays to the end user.

The challenge questions to which the user supplied answers during registration are displayed to the user. The number of questions displayed and the number of correct answers required depends on how the administrator configured the Question and Answer gate.

Lockout Gates

A Lockout Gate is an activity that can be attached to an Authorization Workflow. It is used to determine how many failed password reset attempts can be made before the user is locked out temporarily or permanently. Within a Lockout Gate activity, the administrator can modify:

a) The Lockout Threshold, which is the number of times that a user can fail to answer the minimum number of answers correctly.

b) How long the user is locked out after each Lockout Threshold is reached.

c) The number of Lockout Thresholds that can occur before the user is permanently locked out.

Resetting the password

When all the Question and Answer gates have been successfully completed and verified, the password reset page is displayed to the user, and the new password entered by the user is submitted.

7.5 Policy, user and group management

User management

While users are typically created based on data from HR, users can also be created through the FIM Portal. This permission can be delegated or not delegated to any set of users within FIM.

Self-service user profile management

Users can also be delegated the permission to update some of their own data. Users can either be granted permission to update some attributes of their own data outright, or policies can be configured so that changes to some attributes may require approval by a manager or by HR.

Group management

FIM can be used to manage distribution groups and security groups (whether mail-enabled or not), regardless of scope: Universal, Global, or Domain local. Groups can be configured with more than one owner.

The ability to create groups can be delegated to any set of users within the FIM Portal. Membership in the groups is managed in one of three ways:

a) **Manual.** Members are placed into manually managed groups by the owners of the group. Alternatively, users can request to join a group. The request is either granted automatically or is subject to owner approval. The owners are sent an e-mail message asking them to approve or reject the request.

b) **Manager-based.** A group can also be created that automatically maintains the membership based on who reports to a particular manager. This automatically adds all of the manager's direct reports. If a subsequent import from HR (or another authoritative data source) modifies someone's manager, they are removed from this group and possibly placed in another group. The manager is included in the group as well as their direct reports.

c) **Criteria-based.** Groups based on more advanced criteria can also be created. The criterion is based on attributes and is compared with literal values provided by the group owner. So a group could be based on the following rule, Department is 'Sales.'

Requesting membership in groups

Users can request membership in groups through the FIM Portal, or through the Office Outlook 2007 client. With the FIM Add-in for Outlook installed, users do not need to access the FIM Portal to join and leave distribution lists.

Managing requests

End users can view the status of their own requests to see the current state. End users can also approve or reject requests that are sent to them for approval. Requests are sent to them through e-mail messages and, if using Office Outlook 2010 or Office Outlook 2007 and Exchange 2010 or Exchange 2007, requests can be approved or rejected right from within the e-mail. Additionally, requests for approval can be addressed through the FIM Portal.

Annex A - Defined terms (ASE_REQ)

Term/Acronym	Definition
Action workflow	A workflow that carries out an action after a change to a resource has been committed to the FIM Service database. This includes workflows with activities for sending a notification e-mail message and synchronizing changes to the FIM Synchronization Service database.
Activity	A workflow activity is the basic building block of Windows Workflow Foundation (WF) workflows. It incorporates the logic that is initiated both at design time and run time when building and running workflows.
Approval	An approval is a workflow decision point that can be used to obtain authorization from a person before continuing in the workflow.
Approval threshold	The number of positive approval response messages needed to permit a request to continue processing.
Approver	The person who gives the approval for the request to proceed to the next stage. They receive approval request messages if FIM Add-in for Outlook is used. See also escalation approver.
Attribute flow	This defines the direction in which attribute values flow between the FIM service and other external systems.
Authentication activity	A workflow activity that validates a user's identity. For example, the password reset gate or a smart card authentication gate. See QA gate and lockout gate.
Authentication challenge	A dialog that requires the user to provide a response so that they can authenticate to FIM 2010. For example, questions for the user to answer so that they can reset their passwords.
Authentication challenge activity	A workflow activity that is used to configure a challenge that is issued to a user to authenticate to FIM 2010.
Authorization workflow	A workflow with activities that must be completed before the request is committed to the database. Two examples of activities that could be included in an authorization workflow are a data validation activity and an approval activity.
Destination set (or target resource definition after request)	A set to which a resource moves into because of a request that changes that resource's attributes.
Distribution group	A collection of resources, most commonly users and other groups, to which you can send e-mail messages simultaneously. This is accomplished by sending messages to the mailbox for the group.

Term/Acronym	Definition
Entitlement	A collection of access rights to applications, and other managed resources.
Enumeration	A list of resources returned by the FIM Service.
Escalation	If an approval is not completed within the specified time, the approval is escalated and additional approvers, the escalation approvers, are added to the approval.
Escalation approver	The user who receives approval request messages if an insufficient number of the approvers fail to respond before escalation of the request. See also approver.
Extensible Assertion Markup Language (XAML)	An XML-based language in which workflow definitions are represented.
FIM management agent	A management agent that synchronizes between the FIM Service and the FIM Synchronization Service.
Gate	A workflow activity used in the authentication phase of request processing. See QA gate and lockout gate.
Grant entitlement	The process of adding access rights to applications, directories, and other managed resources.
Lockout	A configuration setting on a person resource in the FIM Service database that restricts that person from authenticating to the FIM Service or performing a password reset.
Lockout gate	A workflow activity in the authentication phase of the request processing intended to lock out a user who has failed to authenticate. See also QA gate and lockout gate.
Lockout threshold	This is an integer control that specifies the number of times a user can fail to complete the authentication workflow before they are locked out for the lockout duration. The default setting for the lockout threshold is 3. The lower limit is 0 and the upper limit is 99.
Lockout duration	This is an integer control that specifies the duration in the number of minutes that the user is locked out after reaching the lockout threshold. The default setting for this is 15 minutes. The lower limit for this setting is 1. The upper limit is 9999, which allows the administrator to set the lockout duration to greater than one day.

Term/Acronym	Definition
Lockout threshold count before permanent lockout	This is an integer control that allows the administrator to configure a numeric value for the number of times a user can reach the lockout threshold before being permanently locked out. Permanent lockout implies that the user must be unlocked by the system administrator. By default, this is set to 3. The range for this setting is between 1 and 99.
Management policy rule	Management policy rules (MPRs) provide a mechanism to model business processing rules for incoming requests to the FIM Service. They control the permissions for requesting operations on FIM Service resources together with the workflows that are triggered by these requests. They also specify the workflows that are triggered by set transitions.
Notification activity	A workflow activity within the action phase of request processing in which the FIM Service sends e-mail messages to one or more users to notify them of the successful completion of a request.
ObjectID (ResourceID)	An attribute that contains a globally unique identifier (GUID) assigned by the FIM Service to each resource when it is created in or synchronized into the FIM Service database. Also known as a resource ID.
Object identifier	A sequence of numbers used as an identifier for a field in a X.509 digital certificate or for an attribute type or object class in an LDAP-based directory service. Object identifiers are typically assigned by software vendors and standards bodies.
Operation type	The operation type is a specification of a type of change to a resource which can be requested through the WS-Transfer web service of the FIM Service. The operation types are creation and deletion of resources, and read, adding values to, removing values from modifying the value of resource attributes.
Operator	An element of a filter that specifies a comparison or another relationship between data values.
Origin set (or target resource definition before request)	A set to which a resource belonged prior to a change in that resource's attributes.
Password reset	A procedure by which a user’s password can be changed to a new value when the user has forgotten or lost their current password. See also registration.

Term/Acronym	Definition
Phase	Each resource creation, update, or deletion request is processed by the FIM Service through three workflow phases. In the authentication phase, additional authentication checks of the requesting user can be performed. In the authorization phase, any necessary approvals are gathered. In the action phase, the activities are performed after the request to change the resource that has been committed.
Policy management	Policy management in FIM 2010 is made possible by a console based on Microsoft Office SharePoint® Server 2007 for policy authoring and enforcement. Extensible workflows based on Windows Workflow Foundation (WF) enable the users to define, automate, and enforce identity management policies. Policy management also includes heterogeneous identity synchronization and consistency that is achieved by the integration of a broad range of network operating systems, e-mail, database, directory, application, and flat-file access.
Precedence	An ordering of synchronization rules.
Requestors	A set used in an MPR to specify the set of resources (usually a set of users) that initiate the MPR evaluation.
QA gate	A workflow activity in an authentication phase in which the requesting user must supply answers to one or more predetermined questions. This activity is typically used in password reset to challenge the user to prove their identity. This challenge is made by prompting the user with a selection of predetermined questions for which only that user would know and for which the user must supply the correct answer. See also lockout gate.
QA challenge	A challenge that requires the user to answer a series of questions in order to authenticate to FIM 2010.
Reference attribute type	An attribute type in which the values of the attribute are the ObjectID (globally unique identifiers) attribute values of other resources in FIM 2010. See also ObjectID.
Registration	A procedure to configure self-service password reset for a user. See also QA gate.
Reregistration	The updating of a registration for an authentication challenge in FIM 2010 typically required after a change to an administrative policy for password reset registration.
Relationship creation	Configuration flags of a synchronization rule that determines whether the resources should be created automatically in FIM 2010 or in the external system, if the resources are absent.
Relationship criteria	Setting of a synchronization rule that is used to match resources in FIM server and resources in external systems.

Term/Acronym	Definition
Relationship termination	Indicates if related resources in other external systems should be disconnected (and perhaps deleted) when the synchronization rule no longer applies.
Request management	The ability for a user to interact with and manage submitted requests and associated workflows.
Requester Management Policy Rule (RMPR)	A management policy rule type that is evaluated and applied against incoming requests to perform operations. RMPRS are primarily used to author access policy definitions in FIM.
Requester or requestor	The identity of the user or service that has submitted a request to FIM 2010.
Resource	An instance of a certain resource type in the FIM 2010. Each resource is uniquely identified by its ObjectID (ResourceID) attribute.
Resource control display configuration (RCDC)	RCDCs are configuration resources that are used to render the UI in the FIM Portal for creating, editing or viewing a resource of a specific resource type in FIM.
Resource hierarchy	In a directory service, the hierarchy of a resource entry is the collection of directory entries between the base of a naming context and that resource entry.
ResourceID (ObjectID)	An attribute that contains a globally unique identifier (GUID) assigned by FIM 2010 to each resource when it is created. Also known as an ObjectID.
Resource scope	A set of resources about which a request can be submitted.
Resource type	A part of a schema that defines the representation of a resource in FIM 2010.
Resource type mapping	A relationship between a resource type used to represent a resource in the FIM Service database and a resource class used to represent that resource in the FIM Synchronization Service metaverse.
Revoke entitlement	The process of removing access rights to applications, directories, and other managed resources.
Role	An organizationally assigned security principal or collection of resources used to manage access rights.

Term/Acronym	Definition
Security descriptor	A structured and associated data that contains the security information for a securable resource. A security descriptor identifies the resource's owner and primary group. It can also contain a discretionary access control list (DACL) that controls access to the resource, and a system access control list (SACL) that controls the logging of attempts to access the resource.
Security principal	An identity used for security management, such as a user account, that can authenticate to a service.
Security token	A protocol element that transfers authentication and authorization information, based on a credential. In the Web services protocols, a security token is represented as an XML element in a SOAP header, as defined by WS-Security.
Security Token Service (STS)	A service that implements the WS-Trust protocol to manage trust between clients and services based on the exchange of security tokens.
Set	A named collection of resources. Typically sets are used to organize resources based on rules. The membership in a set is manually managed or criteria-based. This means that you can manually add resources to a set and that you can define criteria that automatically add resources to a set based on a filter statement. When a resource fulfils the filter criteria, it is automatically added to the related set.
Set Transition management policy rule (TMPR)	A management policy rule that is applied on changes to membership of a set. Set Transition MPRs apply action workflows either when object transition into or out of a specified set in the MPR.
SID	A security identifier (SID). A unique value used to identify a user account, group account, or logon session.
SOAP	Simple Object Access Protocol. A protocol for exchanging structured information between software components.
Synchronization filter	A filter to prevent resources in the metaverse from being transferred to the FIM 2010 database.
Synchronization rule	A rule for flowing resource information between the server running FIM (including the FIM synchronization engine) and connected external system.
Transition Set	A set that is used in a definition of a Set Transition management policy rule. The policy is applied to the changes in the set membership, which can be either objects entering or leaving the set, depending on the TMPR’s configuration.
Timeout	A time period in which FIM 2010 waits for approval responses until the approval activity is escalated.

Term/Acronym	Definition
Web portal	A user interface implemented by a software application through a component of a Web server, such as Internet Information Services (IIS).
Web service	A protocol interface to a service implemented by using an HTTP-based protocol.
Workflow	A workflow is a set of elemental units called activities that are stored as a model that describes a real-world process. Workflows provide a way of describing the order and dependent relationships between work items. This work passes through the model from start to finish, and activities might be performed by people or by system functions.

Annex B - Correspondence and rationale

B.1 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats and OSPs in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.REQUEST	O.REQUEST	Provides direct mapping to the threat and aims to prevent an authenticated user from performing unauthorized actions on stored identity resources.
T.AUTH	O.AUTH	Provides direct mapping to the threat and aims to prevent an unauthorized individual from gaining access to the TOE to performing either unauthorized actions on identity resources or performing unauthorized identity management activities.
T.EXPORT	O.EXPORT	Provides direct mapping to the threat and aims to prevent identity information from being exported outside the scope of control of the TOE in an insecure manner.
T.IMPORT	O.IMPORT	Provides direct mapping to the threat and aims to prevent identity information from being imported from outside the scope of control of the TOE in an insecure manner.
P.SYNCH	O.SYNCH	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability of controlling the flow of identity information.
P.AUTHN	O.AUTHN	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability to implement authentication workflow mechanisms.
P.AUTHZ	O.AUTHZ	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability to implement authorization workflow mechanisms.
P.RESET	O.RESET	Provides direct mapping to the policy statement and aims to ensure that the TOE provides users with the capability to register and perform self-service reset of authentication credentials.

Threats/OSPs	Objectives	Rationale
P.AUTH_FAIL	O.AUTH_FAIL	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability to implement a password reset policy.
P.MANAGE	O.MANAGE	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability to perform the necessary identity management related tasks.
P.ADMIN	O.ADMIN	Provides direct mapping to the policy statement and aims to ensure that the TOE provides administrators with the capability to manage the various security functions and policies of the TOE.
P.DEFAULT	O.DEFAULT	Provides direct mapping to the policy statement and aims to ensure that the TOE provides a default policy rules of deny all for all created identity resource objects.

B.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objectives	Rationale
A.COMMS	OE.COMMS	This IT environment objective provides a direct mapping to the stated assumption and aims to ensure that the communication channels between all server roles are appropriately secured.
A.INSTALL	OE.INSTALL	This operational environment objective provides a direct mapping to the stated assumption and aims to ensure that the TOE is delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.
A.PLATFORM	OE.PLATFORM	This IT environment objective provides a direct mapping to the stated assumption and aims to ensure that the underlying server platform that provides the necessary security capabilities.
A.UNTRUSTED	OE.UNTRUSTED	This operational environment objective provides a direct mapping to the stated assumption and aims to ensure that no untrusted software is installed on the machines the TOE is installed on.
A.NO_EVIL	OE.NO_EVIL	This operational environment objective provides a direct mapping to the stated assumption and aims to ensure that there are suitable administrator resources available to manage the TOE.
A.PROTECT	OE.PROTECT	This operational environment objective provides a direct mapping to the stated assumption and aims to ensure that the TOE and its underlying platform are located within facilities providing controlled access to prevent unauthorized physical access.
A.PATH	OE.PATH	Provides direct mapping to the policy statement and aims to ensure that the TOE provides all remote users with a trusted interface for authenticating to the TOE to ensure the confidentiality and integrity of user and TSF data.

B.3 Dependency rationale

SFR	Dependencies	Rationale
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Included Included
FDP_IFC.1a	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1a	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Included Included
FDP_IFC.1b	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1b	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Included Included
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Included Included Included
FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Included Included
FDP_ITT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Included Included
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.2 included
FIA_UAU.5	No dependencies	-
FIA_UID.2	No dependencies	-
FMT_MSA.1a	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included Included Included
FMT_MSA.1b	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included Included Included

SFR	Dependencies	Rationale
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Not included. Functionality and control of security attributes adequately covered through both FMT_MTD SFRs that specify the TSF data that is controlled by both the user and the administrator. Included
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2 included

B.4 Security functional requirements rationale

The following table demonstrates that all security functional requirements trace back to security objectives of the TOE as specified in the security problem definition.

Objectives	SFRs	Rationale
O.REQUEST	FDP_ACC.1a	This SFR describes one of the base access control policies that relate to the implementation of rules-based policies for FIM 2010. For users or requesters to access resources in the environment, the administrator will need to grant permission to perform operations on them.
	FDP_ACF.1a	FIM access policies are flexible and customizable and the scope is not isolated to just granting permissions, it also permits the implementation of authentication and authorization workflow steps.
O.AUTH	FIA_UID.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
O.EXPORT	FDP_IFC.1b	Outbound synchronization distributes the integrated view of the identity information to all the connected data sources. Outbound synchronization begins in the metaverse and ends in the connector space.
	FDP_IFF.1b	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation and only for those the information is intended for outbound connections.
	FDP_ETC.1	This SFR provides assurance that the TOE user data, identity information, can be transferred securely outside the scope of the TOE to Management Agents and then out to connected identity sources, and Microsoft SQL databases for both the FIM Service Database and the FIM Synchronization Service Database.
O.IMPORT	FDP_IFC.1a	Inbound synchronization creates and updates the integrated view of the identity information from the connected data sources. Inbound synchronization begins in the connector space and ends in the metaverse.

Objectives	SFRs	Rationale
	FDP_IFF.1a	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation and only for those the information is intended for inbound connections.
	FDP_ITC.1	This SFR provides assurance that the TOE user data, identity information, can be imported securely from external identity sources and both the FIM Service Database and the FIM Synchronization Service Database.
O.SYNCH	FDP_ITT.1	This SFR provides assurance that identity information can move from the Management Agent through to the FIM Synchronization Service in a secure manner—free from the threat of disclosure and modification.
O.AUTHN	FIA_UAU.5	This SFR aims to demonstrate that the TOE provides two (2) distinct and separate methods for authenticating users. There is the general user authentication mechanism, which most commonly is the username/password associated with domain credentials and the implementation of a challenge response mechanism to provide users with the ability to reset their domain credentials in the case of forgotten or expired credentials.
O.AUTHZ	FIA_UID.2	The TSF shall require each user to be successfully identified through workflow policies created by the Administrator.
O.RESET	FIA_ATD.1	The TOE will maintain authentication data including the challenge response data necessary for self-service activities.
	FIA_UAU.1	FIM implements a configurable password reset policy that provides the administrator with the capability of establishing a lockout policy that is suitable to the organisation and the operating environment.
	FMT_MTD.1a	The user is capable of performing self-service registration and creating the authentication challenge information required for this step. In addition, the end-user has a certain amount of autonomy and control over their specific identity information.

Objectives	SFRs	Rationale
O.AUTH_FAIL	FIA_AFL.1	FIM implements a configurable password reset policy that provides the administrator with the capability of establishing a lockout policy that is suitable to the organisation and the operating environment.
O.MANAGE	FMT_SMF.1	This SFR provides administrator functionality by the TOE.
O.ADMIN	FMT_MTD.1b	This SFR ensures the administrator is responsible for managing the core TSF data elements that relate to establishing and managing security functional policies for the TOE.
O.DEFAULT	FMT_MSA.3	In FIM, permissions for operations on all objects must be explicitly granted. Unless specifically granted by a management policy rule, all operations on resources are denied.