MQAssure™ NetSignOn Secure Desktop Login

EAL 2 Security Target

Version 1.10

Date: 22nd October 2013

MAGNAQUEST SOLUTIONS SDN. BHD.

Security Target Document for NetSignOn Product Certification under Assurance Maintenance EAL2

Security Target Document

To

Malaysian Common Criteria Evaluation and Certification Schema

By

Magnaquest Solutions SdnBhd.

Malaysia

www.magnaquest.com.my

Version 1.10

22nd October 2013

Document History

Version No.	Date	Revision Description
1.0	1st January 2013	First initial release to evaluator
1.1	7th January 2013	Incorporated changes to" Security Objectives" section.
1.2	3rd April 2013	Incorporated Evaluators Findings
1.3	21st May 2013	Incorporated Evaluators Findings
1.4	18th June 2013	Incorporated changes due to IriShield Camera
1.5	25th June 2013	Incorporated changes in EOR
1.6	25th July 2013	Incorporated changes in EOR
1.7	19th August 2013	Incorporated changes in EOR
1.8	07th October 2013	Incorporated changes in EOR
1.9	16th October 2013	Incorporated changes in EOR
1.10	22nd October 2013	Incorporated changes in EOR

TABLE OF CONTENTS

1 DOCUMENT INFORMATION

1.1 Document Conventions

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text**.
2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*].
3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

1.2 Terminology

Acronym	Meaning
AM	MQAssure™ Access Manager
CC	Common Criteria
EAL	Evaluation Assurance Level
GB	Giga bytes
GHz	Giga Hertz
GINA	The graphical identification and authentication (GINA) library is a component of some Microsoft Windowsoperating systems that provides secure authentication and interactive logon service
GUI	Graphical User Interface
NetSignOn	MQAssure™NetSignOnv3.0 Secure Desktop Login
IAM	MQAssure™ IAM v2.0(may also be referredasIAM)
eKey	eKey is a USB Smartcard token that is used for a two-factor authentication
IM	MQAssure™ Identity Manager

Acronym	Meaning
IP	Internet Protocol. An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication
LAN	Local Area Network
MB	Mega bytes
MHz	Mega Hertz
MyKAD	MyKADis the official compulsory smart identity card of Malaysia. It contains a smart card chip.
Iris	Biometric Iris Image
NTP	Network Time Protocol (a protocol used to synchronize the clocks of computers to sometime reference)
PIN	Personal Identification Number
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	TOE Summary Specification
USB	Universal Serial Bus
User	Staff who uses the TOE

Table 1: Acronyms

Trade marks
"MQAssureTM" is a trademark of Magnaquest Solutions SdnBhd

Titles
Within this document, the following shortened forms of titles may be used:

Magnaquest Solutions SdnBhd - 'Magnaquest'
MQAssure™ NetSignOn v3.0 – MQAssure™NetSignOn

1.3 References

- Common Criteria Part 1 Version 3.1 Revision 4

- Common Criteria Part 2 Version 3.1 Revision 4
- Common Criteria Part 3 Version 3.1 Revision 4
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 4

1.4 Document Organization

This ST contains:

- TOE Description: Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- Security Objectives: Identifies the security objectives that are to be satisfied bythe TOE and TOE environment.
- TOE Security Functional Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE.
- TOE Security Assurance Requirement: Presents the Security Assurance Requirements (SARs) met by the TOE.
- TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives.

2 SECURITY TARGET INTRODUCTION

2.1 ST and TOE Reference

ST Title	MQAssure™ NetSignOnv3.0 Secure Desktop Login
ST Version	Version 1.10
ST Publication Date	22nd October 2013
TOE Identification	MQAssure™ NetSignOn v3.0
TOE Version	Version 3.0
CC Identification	CC Version 3.1 Revision 4
Assurance Level	EAL 2
ST Author	Vinay Kumar Tiruvaipeta
Keywords	NetSignOn

Table 2: TOE Reference

2.2 TOE Overview

MQAssure™ NetSignOn v3.0 Secure Desktop Login is a client agent that integrates with Windows operating system platforms of the desktops and laptops. It leverages multiple authentication methods such as MyKAD, biometric (Fingerprint/Iris), USB token, and userid/password to perform the login functionality to a system in a Domain (Network connected mode and network disconnected mode).

MQAssure™ NetSignOn v3.0 provides the following security features that are described in Section 2.3.1. Briefly, the security features introduced by the TOE are:

1. User data protection
2. Identification and authentication
3. Security management

2.2.1 TOE Type

MQAssure™ NetSignOn v3.0 is a client agent that runs on Windows operating systems. The TOE only covers MQAssure™ NetSignOn v3.0 that runs in system connected to domain. It supports multifactor user authentication to the workstations. Please refer to section 2.3.1 for the logical scope of the TOE.

2.2.2 Hardware and Software Required by the TOE

Below are the requirements for the hardware and software to run the TOE:

No.	Requirement	Version / Specification
1	Client Token	• USB Token (For evaluation purpose, eKey with 72KB is used) • E-ID Smart Card (For evaluation purpose, MyKAD-Malaysian Identity Card is used) • Biometric Reader (finger print) (For evaluation purpose, CID308 is used) • Biometric Reader (Iris) (For Evaluation purpose, Iritech IriTerminal BD300F device is used)
2	Operating System / Software	• For MQAssure™ NetSignOn v3.0 client ▪ Windows XP (32 bit) ▪ Windows Vista (32 bit) ▪ Windows 7 (32 bit) ▪ Also, requires the following software: • Iris BCR 200 DTP Finger print reader driver (for reading MyKAD) • eKey smart card reader driver (for using eKey) • Internet Explorer 9.0, Google Chrome 23.0, Mozilla Firefox 17.0 latest Versions (for accessing IAM web application) • IriShield-USB MK2120U iris reader driver • For IAM Server ▪ Windows 2008 Enterprise Edition with service pack 2 or above ▪ Also, requires the following software: • MySQL 5.0 database • Glassfish 2.1 application server • Tomcat Server 5.5.9 • J2SE Development Kit 5.0 Update 6 • Internet Explorer 9.0, Google Chrome 23.0, Mozilla Firefox 17.0 latest Versions (for accessing IAM web application) • For Directory Server ▪ Windows Server 2008 Enterprise Edition with service pack 2 or above ▪ Also, requires the following software; • Active Directory (LDAP compliant)
	Hardware	• For MQAssure™ NetSignOn v3.0 client ▪ Pentium or higher with 1GHz or higher, with at least 1 GB of RAM ▪ PS/2 keyboard or mouse port ▪ Microsoft mouse or compatible pointing device ▪ A CD-ROM drive, unless installation can be done via the network ▪ VGA or higher resolution graphic card ▪ TCP-IP protocol that is properly configured ▪ A USB port (if eKey is to be used as the authentication token) ▪ IRIS BCR 200 DTP MyKAD reader (if MyKAD is to be used as the authentication token)

No.	Requirement	Version / Specification
		▪ IRIS BCR 200 DTP fingerprint Biometric reader with Sagem finger print sensor (if finger print is to be used along with MyKAD) ▪ Irishield Mono 2120 Iris Biometric Reader with Iris Capture Camera (if Iris based Authentication is used) • For IAM Server ▪ Intel Core2 Duo or higher with 2GHz or higher, with at least 4 GB of RAM ▪ PS/2 keyboard or mouse port ▪ Microsoft mouse or compatible pointing device ▪ A CD-ROM drive, unless installation can be done via the network ▪ VGA or higher resolution graphic card ▪ TCP-IP protocol that is properly configured • For Directory Server ▪ Intel Core2 Duo or higher with 2GHz or higher, with at least 1 GB of RAM ▪ PS/2 keyboard or mouse port ▪ Microsoft mouse or compatible pointing device ▪ A CD-ROM drive, unless installation can be done via the network ▪ VGA or higher resolution graphic card ▪ TCP-IP protocol that is properly configured

Table 3: Hardware & Software Requirements

Notes:

1. The mentioned hardware and software requirements are not part of the TOE.
2. All mentioned 3rd party software is not part of the TOE.

2.3 TOE Description

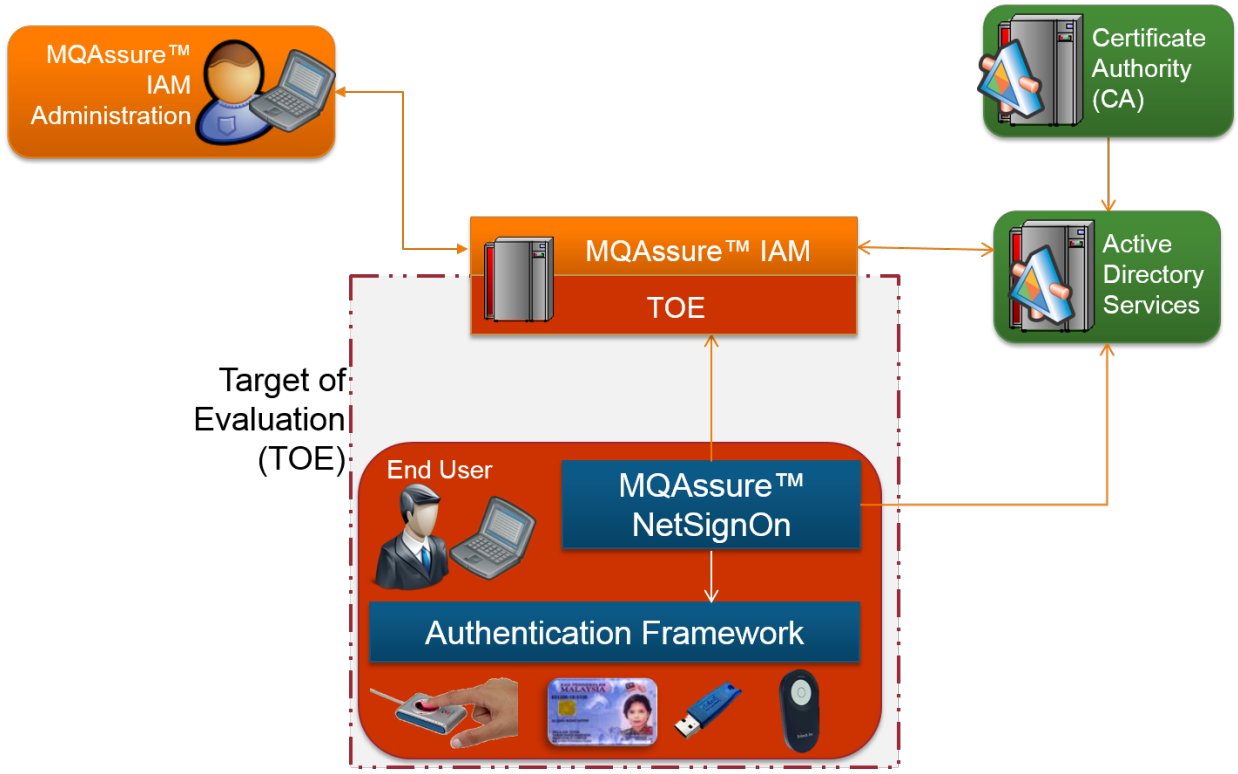

Figure 1: MQAssure™NetSignOnArchitecture

Figure 1 depicts the architecture of MQAssure™ NetSignOn v3.0. It has the following components.

1. MQAssure™ IAM v2.0 (or IAM)

IAM is a centralized identity and access management platform. It provides the backbone for the MQAssure™ NetSignOn v3.0 by providing centralized policy management (part of IM), session management and audit logging (part of AM). In the overall infrastructure MQAssure™ NetSignOn v3.0 acts as a policy enforcement agent for workstations. IAM provides a centralized administration console through which the administrators can create and enforce various policies to control the authentication schemes to workstations in a domain. IAM consists of the following modules:

a. MQAssure™ Access Manager (AM) that is partially in scope of the TOE, which is where the run-time (real-time) checks are performed during the authentication phase.
b. MQAssure™ Identity Manager (IM) is where administrators would define the authentication policy and viewing of reports. The Self-help function within IM (that is available to the TOE users) is within the scope of the TOE, remaining part of the IM is not part of TOE
c. Admin Module that is also not in scope of the TOE, which is where the *administrators would use to connect to IM for policy definition and self help*

2. Active Directory Services.

An active directory (AD) is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. It also stores user account details and

workstations details joined in to a domain. User information is synchronized between the databases in IAM and AD. The synchronization of the databases will be done manually during the initial setup. Subsequently, the databases will be synchronized automatically for any changes to the user information. AM will verify the userid and password during the authentication phase with the AD server. This part is not in the scope of the TOE

3. Windows Certificate Authority on AD Server (Windows CA)

A certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes. The Windows CA digital certificate is used to authenticate the AD server to the IAM server. This part is not in the scope of the TOE

4. MQAssure™ NetSignOn v3.0

MQAssure™ NetSignOn v3.0 is implemented as a custom GINA (Dynamic Link Library) in Windows XP and as credential provider in later versions of Windows. This provides the login interface to the users to login to their respective workstations. MQAssure™ NetSignOn v3.0 makes use of the MQAssure™ IAM2.0 services to select appropriate authentication scheme and retrieve the credentials for that particular user.

The credentials that are checked at the AM during the authentication phase include user authentication scheme, token numbers such as eKey serial number, MyKAD number, PIN / password with MyKAD, iris biometric image and passwords. PIN for the eKey is internally stored in the token and biometric reference is stored in the MyKAD itself.

The following diagram illustrates the process of logging into system in domain using MQAssure™ NetSignOn v3.0;

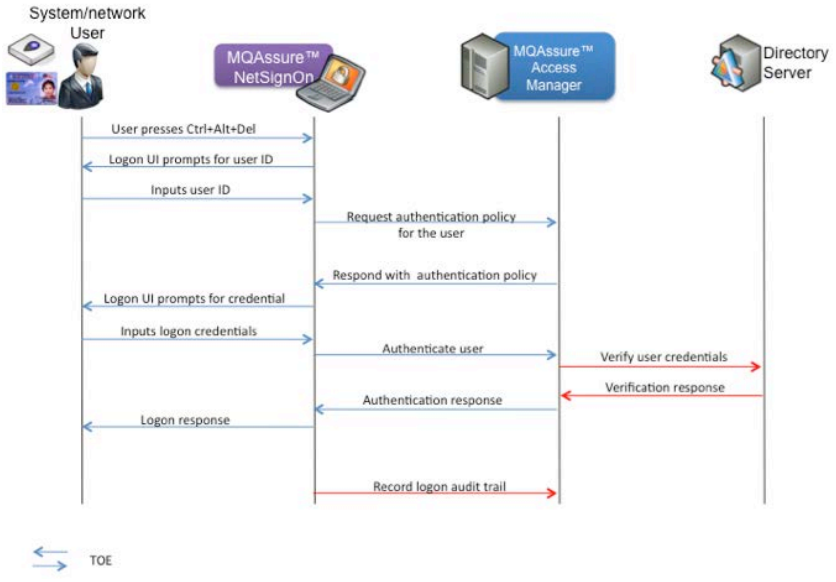

Figure 2: MQAssure™ NetSignOn Process

Note from the above figure (Figure 2) that:

1. The TOE is only for the usage of MQAssure™ NetSignOn v3.0 within a network environment.
2. The Directory Server is not part of in scope of the TOE. However, the server is required for the usage of the TOE in a network environment.

Users can login through one of the following of authentication methods:

1. Userid/password: Users are assigned with usernames and passwords to login to the system / network.
2. MyKAD/PIN: Users can login to the system / network by inserting their MyKAD into the reader and then type in their PIN
3. MyKAD/Biometric: Users can login to the system / network by inserting their MyKAD into the reader and then place their finger onto the fingerprinting reader
4. eKey/PIN: Users can login to the system / network by inserting their eKey into the USB reader and then type in their PIN
5. Iris Biometric Image: Users can login to the system / network by verifying Iris image with the iris biometric reader.

The following management functions are not part of the TOE:

1. Registration or enrollment of users into IAM
2. Enrollment of user credentials with MyKAD or eKey
3. Synchronization of the IAM and AD databases
4. Verification of userid and password at the AD server
5. Policy configuration in IAM and AD servers
6. MQAssure™ NetSignOn Licensing implemented in IAM.
7. The Self-help function within IAM for IAM administrators

2.3.1 Scope of the TOE

Below is the TOE scope description for the identified security functions. The details can be found in the TSS section.

Security Function	TOE Scope Description
User Data Protection	The users can login to the domain via one of the following methods: Userid and password combination, or MyKAD and PIN/password combination, or MyKAD and Biometric (finger printing) combination, or eKey and PIN combination, or iris Biometric image. Userid and password combination must be combined with either MyKAD or eKey or iris biometric authentication scheme. Regardless of the authentication mechanism used, the initial userid must be entered at the very beginning of the authentication process. Users are required to login through one of the above combinations from a locked out or logged out state. Note that the locked out state is defined as when the users of IM has reached the maximum number of allowable login trials whether the authentication has failed. The logged out state is defined as when the users of IM or MQAssure™ NetSignOn v3.0 component choose to log out.

Security Function	TOE Scope Description
Identification and Authentication	Users must be identified and authenticated before access to relevant resources is allowed. The user identities, type of authentication scheme (like via eKey or MyKAD or Iris Biometric), the user credentials and roles are maintained. If a user authentication scheme is done via a combination of userid and password, the TSF verifies the password to ensure that it includes both alpha and numeric characters, contains at least one complex character, and does not contain repeating predictable sequence. The password must also adhere to the minimum number of characters. User account will be locked after several unsuccessful authentication attempts.
Security Management	The users are allowed to login to the domain, as well as change their associated passwords. The users can change the passwords using IM or through MQAssure™ NetSignOn v3.0 user Application. There are 3 different reasons for users to change passwords. Refer to TSS for details. There are 2 types of PINs. The first type, which is the PIN / password used with MyKAD can be changed using IM or MQAssure™ NetSignOn v3.0 user application. The second type, which is the PIN for eKey, can be changed via the eKey software itself since it's stored in the eKey itself .eKey and its related software are not part of the TOE. User accounts are locked after a number of unsuccessful authentication attempts (default is 3 attempts)in IM. And, users must be re-authenticated through the security questionnaire once their account is locked to unlock their account.

Table 4: Logical Scope

3 CONFORMANCE CLAIMS

3.1 Common Criteria Claims

The following conformance claims are made for the TOE and ST:

- **CCv3.1 Rev.4 conformant**. The TOE and ST are Common Criteria conformant to Common Criteria version 3.1 Revision 4.
- **Part 2 conformant**. The ST is Common Criteria Part 2 conformant.
- **Part 3 conformant**. The ST is Common Criteria Part 3 conformant.
- **Package conformant**. The ST package is conformant to Evaluation Assurance Level (EAL) 2.
- The TOE and ST does not conform to **Protection Profiles**.

4 SECURITY PROBLEM DEFINITION

4.1 Introduction

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

- Known and presumed threats countered by either the TOE or by the TOE environment;

- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects
- Organizational Security Policies that consist of rules or guidelines that must be followed by the TOE and/or its operational environment.

4.2 Threats

The TOE address the following threats listed in Table 5 below.

Identifiers	Description
T.Attack_Desktop	An attacker may gain access to a desktop.
T.Attack_Userdata	An attacker may gain access to User data.
T.Access_Desktop	A desktop user may gain unauthorized access to a desktop.
T.Access_Userdata	A desktop user may gain unauthorized access to another desktop user's User data.
T.Intercept	An attacker may intercept communication channels. This may lead to compromise of users' authentication credentials, other User data, or Configdata in transit.
T.Spoof	An attacker may cause communications between a User Device and a server to be redirected, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead to compromise of users' authentication credentials.
T.Mod_Conf	An attacker or authorized user may modify a user's configuration. This covers: • modification of the user's set of permitted applications /actions • Modification of configuration data associated with a user.

Table 5: Threats addressed by the TOE

4.3 Organizational Security Policies (OSPs)

TOE will execute under the context of underlying OSP. This section describes all the security policies that the organization follows to protect the TOE.

Identifiers	Description
P.Role	Only authorized individuals that are assigned by the organization have access to the TOE.
P.Credential	User shall not disclose any credential information towards other users.

Table 6: Organizational Security Policies (OSPs)

4.4 Assumptions

The TOE address the following Assumptions listed in Table 7 below.

Identifiers	Description
A.Physical	It is assumed that TOE servers are installed in a physically secure location that can only be accessed by authorized administrators.
A.Trust_Admin	Administrators are trustworthy.
A.Third_Party_SW	Trusted third party software is operating correctly and securely. Trusted third party software is defined as: • Web Browsers used to connect • Windows Server 2008 (including Active Directory) • Firewall software (Note: This, in fact, includes Firewall hardware too) • Microsoft Server 2008 Certificate Services • eKey Smartcard software • Iritech Iris BD300F Device Software
A.Operations_Security	Where keys and other secret data are generated and stored outside the TOE, they are managed in accordance with the level of risk.
A.Config	The Configurations used remained unchanged and unaffected by other applications

Table 7: Assumptions addressed by the TOE

5 SECURITY OBJECTIVES

5.1 Security Objective for the TOE

Certain objectives with respect to the TOE must meet its security functional requirements. Those objectives are:

Security Objective	Description
OT.AUTH_USER	Desktop users must be successfully identified and authenticated for being granted access to the TOE.
OT.AUTH_SERVER	TOE server components must authenticate themselves with the Client before communication of Userdata or Configdata.

Security Objective	Description
OT.DESKTOP	Desktop users must be granted access only to desktops for which they have been authorized.
OT.ROLES_AND_ACCESS	The TOE shall limit the restricted functionality to those authorized and authenticated. The TOE administrator shall be the only one to authenticate to the TOE administration functionality in MQAssure™ IAM v2.0
OT.SECURE_AUTH	The TOE must provide a biometric (Iris/Fingerprint) or Smartcard (MyKAD or eKey) verification mechanism to ensure access to the TOE.
OT.APPS_AVAIL	Authorized users must have access to the permitted applications.

Table 8: Security Objectives for the TOE

5.2 Security Objective for the Operational Environment

Certain objectives with respect to the general operating environment must be met for the TOE to meet its security functional requirements. Those objectives are:

Security Objective	Description
OE.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains the organizational IT security objectives.
OE.RELIABLE	All hardware and third party software supporting the TOE are reliable and operating in good condition. All client tokens (MyKAD and eKey) are reliable and operated in a secure manner. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. All supporting components' performance is monitored and maintained by administrators.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.
OE.COMM	The TOE environment ensures secure communications of security relevant data from and to the TOE.
OE.CONFIG	The user registration in IAM, configuration and security settings of the entire suite of IAM must be performed prior to the usage of the TOE.
OE.DB	The TOE environment must provide the database of the network users in a directory server.

Security Objective	Description
OE.PIN	The person responsible must ensure the correctness of user information in the smart card and USB token.
OE.SYNC	The password policy, user credential information and other type of information within IAM and AD servers must be synchronized at all times.
OE.ATTMP	The number of unsuccessful login attempts to the domain is based on the policy within the AD.
OE.PHYSICAL	The operational environment of the TOE restricts the physical access to the TOE to only authorized personnel.

Table 9: Security Objective for the Operational Environment

5.3 Security Objectives Rationale

The following table provides a summary of the relationship between the security objectives and the security problem definition. The rationale is provided in the sections that follow.

Threat / Assumptions / Security Objective	T.Attack_Desktop	T.Attack_Userdata	T.Access_Desktop	T.Access_Userdata	T.Intercept	T.Spoof	T.Mod_Conf	A.Physical	A.Trust_Admin	A.Third_Party_SW	A.Operations_Securi	A.Config	P.Role	P.Credential
OT.AUTH_USER			X	X										
OT.AUTH_SERVER			X	X				X						
OT.DESKTOP			X										X	
OT.ROLES_AND_ACCESS			X									X	X	
OT.SECURE_AUTH			X							X				
OT.APPS_AVAIL				X										
OE.NOEVIL		X									X			
OE.INSTALL	X								X	X		X		
OE.RELIABLE								X		X	X			
OE.CREDEN	X	X	X	X		X	X		X					X
OE.COMM		X			X	X								

Threat / Assumptions / Security Objective	T.Attack_Desktop	T.Attack_Userdata	T.Access_Desktop	T.Access_Userdata	T.Intercept	T.Spoof	T.Mod_Conf	A.Physical	A.Trust_Admin	A.Third_Party_SW	A.Operations_Securi	A.Config	P.Role	P.Credential
OE.CONFIG			X			X	X					X		
OE.DB		X												
OE.PIN											X			
OE.SYNC	X								X					
OE.ATTMP	X	X	X											
OE.PHYSICAL	X							X					X	

Table 10: Threats/Assumptions/OSPs addressed by Security Objectives for the TOE

5.3.1 T.Attack_Desktop

Attackers are prevented from gaining access to a desktop of TOE to apply identification and authentication.

OE.CREDEN will ensure that only identified and authenticated desktop users and administrators are granted access to the TOE.

OE.INSTALL will ensure secure installation of TOE by local system administrator.

OE.SYNC will ensure that all the policies and authentication details/updates are synchronized with IAM server.

OE.PHYSICAL will ensure that only authorized personnel are accessing the TOE.

OE.ATTMP will ensure that any unauthorized trails to access the TOE will lock the user account.

5.3.2 T.Attack_Userdata

Attackers are prevented from gaining access to User Data by secure communication channels, secure installation process and storage of configuration / user data in a secure manner.

OE.NOEVIL will ensure properly trained authorized persons will do the installation and configuration actions of the TOE.

OE.CREDEN will ensure that only identified and authenticated desktop users and administrators are granted access to the user data.

OE.COMM will ensure secure SSL communication happens when the TOE interacts with Server.

OE.DB will ensure secure storage of data in the server Database.

OE.ATTMP will ensure that any unauthorized trails to access the user data will lock the user account.

5.3.3 T.Access_Desktop

This prevents unauthorized users from accessing the desktops.

OE.CREDEN, OT.DESKTOP, OT.ROLES_AND_ACCESS, OT.SECURE_AUTH, OT.AUTH_SERVER and OT.AUTH_USER will ensure that only identified and authenticated desktop users and administrators are granted access to their particular assigned desktops.

This ensures only authorized users registered with the desktops are permitted to access their desktops.

Proper Audit trails are maintained to verify the user actions.

OE.CONFIG will specify the users registered with corresponding Desktops with particular authentication schemas.

OE.ATTMP will ensure that any unauthorized trails to access the user data will lock the user account.

As only Authorized system administrator are allowed to access the Server. So Unprivileged or Unauthorized users are not allowed to access server. Only after Successful authentication to the Server Machine, the administrator can access IAM server.

5.3.4 T.Access_UserData

OE.CREDEN, OT.APPS_AVAIL, OT.AUTH_SERVER, and OT.AUTH_USER will ensure that users registered with the desktops can be authorized for access to desktops and Data.
Only after successful authentication of the server through OT.AUTH_SERVER the admin can access server and access the user data by authentication to the IAM.

5.3.5 T.Intercept

Attackers are prevented from intercepting communications channels of TOE to apply authentication, confidentiality and integrity.

OE.COMM will ensure secure SSL communication while interacting with Server.

5.3.6 T.Spoof

Attackers are prevented from redirecting communications happening with server to a spoof server of TOE to apply authentication, confidentiality and integrity.

OE.CREDEN and OE.COMM ensure that servers authenticate themselves to clients before communicating User data such as authentication credentials.

OE.CONFIG ensures that the servers, User Devices have been set up properly.

5.3.7 T.Mod_Conf

Attackers and desktop users are prevented from modifying Configdata of TOE to apply authentication, authorization, confidentiality and integrity.

OE.CREDEN ensures that

- Only identified and authenticated desktop users and administrators are granted access to the TOE.
- Only administrators have access to Configdata
- Confidentiality and integrity checks of the Configdata on the servers and when transmitted between servers.

OE.CONFIG ensures that the servers have been set up properly and potentially privileged programs do not undermine security

5.3.8 A.Physical

The assumption that TOE servers are installed in physically secure locations is addressed by the environment objective OE.RELIABLE and OE.PHYSICAL which ensures that servers are physically protected and only accessible by administrators.

5.3.9 A.Trust_Admin

The assumption that Administrators are always trusted is identified by the OE.CREDEN, OE.INSTALL and OE.SYNC, which ensures and identifies the admin users.

5.3.10 A.Third_Party_SW

The assumption that third party software is operating correctly and securely is met by the environment objectives OE.RELIABLE which ensures that trusted third party software is securely configured, and OE.INSTALL and OT.SECURE_AUTH which ensures that only securely configured trusted third party software is installed on the User Systems.

5.3.11 A.Operations_Security

The assumption that secret data outside the TOE is managed appropriately is met by environment objective OE.PIN and OE.RELIABLE which ensures that keys and other secret data generated and stored outside the TOE are managed in accordance with the level of risk. OE.NOEVIL will ensure proper installation and Configuration of the TOE Operations.

5.3.12 A.Config

The assumption that configuration remains unchanged and unaffected by other applications is ensured by OE.INSTALL and OE.CONFIG.

5.3.13 P.Role

OT.DESKTOP and OT.ROLES_AND_ACCESS will ensure that only identified and authenticated desktop users and administrators are granted access to their particular assigned desktops
OE.PHYSICAL will ensure that only authorized personnel has physical access to the TOE.

5.3.14 P.Credential

OE.CREDEN ensures that users are disallowed to disclose any credential information related to the TOE such as password and so on. Users need to comply with the organization security policy implemented in the TOE operational environment.

6 SECURITY REQUIREMENTS

This section specifies the requirements for the TOE.

6.1 TOE Security Functional Requirements (SFRs)

This section specifies the SFRs for the TOE. It organizes the SFRs by the CC classes.

Requirement Class	Requirement Component
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UAU.6: Re-authenticating
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security Roles

Table 11: TOE Security Functional Requirements

6.1.1 User Data Protection

6.1.1.1 Subset Access Control (FDP_ACC.1)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [access control policy] on [users logging into the domain on MQAssure™ NetSignOn v3.0 by performing the run-time check at the IAM level].

6.1.1.2 Security attribute based access control (FDP_ACF.1)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset Access Control
FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1 The TSF shall enforce the [access control policies] to objects based on the following: [

a) User identity (userid)
b) Type of the authentication scheme assigned
c) Credential for the assigned authentication scheme
    i. PIN / Password for either userid or MyKAD
    ii. MyKAD number
    iii. Biometric reference for MyKAD
    iv. PIN for eKey
    v. Serial number for eKey
    vi. Iris biometric image for Iris Authentication
d) Role].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Upon receiving user request to access the domain from a logged out state or locked out state. These rules also cover user request to access the domain on initial authentication. The rules are:

a) If the assigned authentication scheme for the user is MyKAD and PIN / password, then the user is prompted to insert his MyKAD into the reader and provide the PIN / password
b) If the assigned authentication scheme for the user is MyKAD and Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner
c) If the assigned authentication scheme for the user is eKey and PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN
d) If the assigned authentication scheme for the user is Iris Biometric, then the user is prompted for Iris image on the Iris Biometric Reader.
e) If the assigned authentication scheme for the user is userid and password, then the user is prompted to enter his password].

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].

6.1.2 Identification and Authentication

6.1.2.1 Authentication failure handling (FIA_AFL.1)

Hierarchical to: No other components.

Dependencies:FIA_UAU.1 Timing of authentication

FIA_AFL.1.1: The TSF shall detect when[*an administrative configurable positive integer within 1 to 99*] for unsuccessful authentication attempts occurred related to [authentication pagein IM].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [lock the user account].

Application Note: *Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency. The default number of unsuccessful attempts is 3.*

6.1.2.2 User attributes definition (FIA_ATD.1)

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 identity (userid)
b) Type of the authentication scheme assigned
c) Credential for the assigned authentication scheme
    i. PIN / Password for either userid or MyKAD
    ii. MyKAD number
    iii. Biometric reference for MyKAD
    iv. PIN for eKey
    v. Serial number for eKey
    vi. Iris Biometric reference for Iris
d) Role].

6.1.2.3 Verification of secrets (FIA_SOS.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1: The TSF shall provide a mechanism to verify that secrets meet [the following quality checks for TOE user PIN / password:

a) Must include numeric characters
b) Contain at least one complex character
c) Must not contain repeating predictable sequence
d) Must contain a minimum number of characters]

Application Note: *This SFR is relevant for the changing of PIN / passwords in IM. This SFR does not apply to the PIN stored in the eKey.*

6.1.2.4 User authentication before any action (FIA_UAU.2)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies:FIA_UID.1 Timing of identification

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.

Application Note: *Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.*

6.1.2.5 Multiple authentication mechanisms (FIA_UAU.5)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1: The TSF shall provide [a mechanism to accept authentication scheme within MQAssure™ NetSignOn component in the form of:

a) userid and password
b) userid, MyKAD, and Biometrics
c) userid, MyKAD, and PIN / Password
d) userid, eKey USB Token, and PIN
e) userid, Iris biometrics]

To support user authentication.

FIA_UAU.5.2: The TSF shall authenticate any user's claimed identity according to the [authentication policy of the MQAssure™ NetSignOn component such that userid must be entered prior to one of the following authentication scheme:

a) If the assigned authentication scheme for the user is MyKAD and PIN / password, then the user is prompted to insert his MyKAD into the reader and provide the PIN / password
b) If the assigned authentication scheme for the user is MyKAD and Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner
c) If the assigned authentication scheme for the user is eKey and PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN
d) If the assigned authentication scheme for the user is Iris Biometric, then the user is prompted for Iris Biometric image.
e) If the assigned authentication scheme for the user is userid and password, then the user is prompted to enter his password].

6.1.2.6 Re-authenticating (FIA_UAU.6)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1: The TSF shall re-authenticate the user under the conditions [

a) System locked
b) System logged out].

6.1.2.7 User identification before any action (FIA_UID.2)

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

6.1.3 Security Management

6.1.3.1 Management of security attributes (FMT_MSA.1)

Hierarchical to: No other components.

Dependencies: [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

FMT_MSA.1.1: The TSF shall enforce the [access control policy] to restrict the ability to [*change_default*] the security attributes [password for userid, and PIN / password used with MyKAD Authentication Schema] to [TOE users].

Application Note: *The users can change the PIN / passwords inIM or MQAssure™ NetSignOn User Application for userid or MyKAD authentication scheme.*

6.1.3.2 Static attribute initialisation (FMT_MSA.3)

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 [access control policy] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the [TOE users] to specify alternative initial values to override the default values when an object or information is created.

6.1.3.3 Specification of management functions (FMT_SMF.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Change passwords for userid
b) Change PIN / password for MyKAD Authentication Schema].

6.1.3.4 Security roles (FMT_SMR.1)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1:	The TSF shall maintain the roles [TOE users].
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.
Application Note:	*Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.*

6.2 TOE Security Assurance Requirement

The TOE meets the security assurance requirements for EAL2. The following table is the summary for the requirements:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security Architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic Design
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance AGD_PRE.1 Preparative Procedures
ALC: Life-cycle support	ALC_CMC.2 Use of the CM System ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery Procedures
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.2Derived security requirements ASE_SPD.1 Security Problem Definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional Testing ATE_IND.2 Independence Testing – Sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 12: TOE Security Assurance Requirements

6.3 Security Requirement Rationale

The following table provides a summary of the relationship between the security Functional Requirements and the TOE security Functions. The rationale is provided in the sections that follow.

TOE Security Function / Security Functional Requirements	OT.AUTH_USER	OT.AUTH_SERVER	OT.DESKTOP	OT.ROLES_AND_ACCESS	OT.SECURE_AUTH	OT.APPS_AVAIL
FDP_ACC.1	X	X	X	X		
FDP_ACF.1	X	X	X	X		
FIA_AFL.1	X	X	X		X	
FIA_ATD.1	X	X	X		X	
FIA_SOS.1	X	X	X		X	
FIA_UAU.2	X	X	X		X	X
FIA_UAU.5	X	X	X		X	
FIA_UAU.6	X	X	X		X	
FIA_UID.2	X	X	X			X
FMT_MSA.1				X	X	
FMT_MSA.3				X	X	
FMT_SMF.1				X	X	
FMT_SMR.1				X	X	

Table 13: TOE Security Objectives realized by the security function requirements

6.3.1 OT.AUTH_USER

TOE users need to authenticate with their credentials using the authentication Schema assigned to them to get access to the desktop or IAM Server.

Unauthorized users are not permitted to access the resources.

6.3.2 OT.AUTH_SERVER

Authorized Users are permitted to access the IAM Server. IAM users need to authenticate themselves with the IAM server with their authentication credentials.

6.3.3 OT.DESKTOP

TOE specifies the secure authentication mechanism to authenticate the user to access his / her Desktop. Only after successful authentication by the User the access to Data or application or Desktop is permitted.

6.3.4 OT.ROLES_AND_ACCESS

FDP_ACC.1 and FDP_ACF.1functional requirements implementation gives the complete flow of access control for the users.
MQAssure™ NetSignOn enforces access control policy for users to login with one of the secure authentication mechanism that is configured in IAM and approved by IAM administrator.

FMT_SMR.1 and FMT_SMF.1implementation ensures that a role based access and actions can be performed.

6.3.5 OT.SECURE_AUTH

FIA_AFL.1 functional specification enhances security provided by limiting the Unsuccessful authentication attempts by the user.

FIA_SOS.1 improves the complexity of the password to be assigned by user by implementation of a password policy mechanism.

FIA_ATD.1, FIA_UAU.2, FIA_UAU.5 and FIA_UAU.6 functional implementation with allow enhancing the authentication mechanism by providing multiple authentication schemas, re authenticating the user after logout/logoff and will allow access to the application only after successful authentication.

6.3.6 OT.APPS_AVAIL

The access to the available data or application is only permitted after successful authentication with one of the secure authentication mechanism.

FIA_UAU.2 & FIA_UID.2 functional Implementation permits users to access data or application only after successful authentication.

7 TOE SUMMARY SPECIFICATION

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST. Each of the security requirements and the associated descriptions correspond to the security functions. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

7.1 TOE Security Functions

7.1.1 User Data Protection

No.	SFR	Description
1	FDP_ACC.1	MQAssure™ NetSignOn enforces the access control policy based where the users can login to the domain using one of the following authentication schemes: 1. Userid and password combination 2. Userid, MyKAD and PIN / password combination. 3. Userid, MyKAD and Biometric (finger printing) combination 4. Userid, eKey and PIN combination 5. Userid, Iris Biometric combination Users are required to login through one of the above combinations from a locked out or logged out state. The users must first press Ctrl-Alt-Del prior to the authentication to the domain using the defined authentication scheme above. These authentication schemes supported for MQAssure™ IAM Web Login is also managed within the MQAssure™ IAM.
2	FDP_ACF.1	The access control policy in the MQAssure™ IAM 2.0 will check on the following objects to ensure that users are properly identified and authenticated: a) User identity (userid) b) Type of the authentication scheme assigned c) Credential for the assigned authentication scheme i. PIN / Password for either userid or MyKAD ii. MyKAD number iii. Fingerprint Biometric reference for MyKAD iv. Iris Biometric reference for Iris v. PIN for eKey vi. Serial number for eKey d) Role: User and administrator (not part of the scope). Refer explanation in FMT_SMR.1 for more details. If the assigned authentication scheme for the user is MyKAD and PIN / password, then the user is prompted to insert his MyKAD into the reader and provide the PIN / password. If the assigned authentication scheme for the user is MyKAD and

No.	SFR	Description
		Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner. If the assigned authentication scheme for the user is Iris then the user is prompted for Iris Biometric Image. If the assigned authentication scheme for the user is eKey and PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN. If the assigned authentication scheme for the user is userid and password, then the user is prompted to enter his password.

Table 14: TSS for User Data Protection

7.1.2 Identification and Authentication

No.	SFR	Description
1	FIA_AFL.1	The user accounts are locked after a defined number of unsuccessful authentication attempts when users log in to IM. And, users must be re-authenticated once they are either locked or logged out of the domain. The number of unsuccessful attempts is set by the administrator in IM (this process is not part of the TOE). The default value is 3, however it can be set as an integer value between 1 to 99.
2	FIA_ATD.1	The following user attributes are maintained for each authenticated users: a) User identity (userid) b) Type of the authentication scheme assigned c) Credential for the assigned authentication scheme i. PIN / Password for either userid or MyKAD ii. MyKAD number iii. Biometric reference for MyKAD iv. Iris Biometric reference for Iris v. PIN for eKey vi. Serial number for eKey d) Role: User and administrator (not part of the scope). Refer explanation in FMT_SMR.1 for more details.
3	FIA_SOS.1	By default, user password will be the same as userid. At first time login and authenticated to IAM, the user is enforced to change the default password. The TSF verifies the entered PIN / password during changing password to ensure that it includes numeric characters, contains at least one complex character, and does not contain repeating predictable sequence. The password must also adhere to the minimum number of characters. This run-time (real-time) check is performed during the authentication process by AM. The password policy above is set by an administrator in IM (this

No.	SFR	Description
		process is not part of the TOE).
4	FIA_UAU.2& FIA_UID.2	Users can only access the TOE (MQAssure™ NetSignOn v3.0 component and IM component for password management) once they are identified and authenticated. The identification and authentication to the MQAssure™ NetSignOn v3.0 component is accomplished via one of the following methods: 1. If the assigned authentication scheme for the user is MyKAD/PIN (or password), then the user is prompted to insert his MyKAD into the reader and provide the PIN / password after entering the userid 2. If the assigned authentication scheme for the user is MyKAD/Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner after entering the userid 3. If the assigned authentication scheme for the user is eKey/PIN, then the user is prompted to insert his eKey into the USB port and provide the PIN after entering the userid 4. If the assigned authentication scheme for the user is Iris based, then the user is prompted for Iris Biometric after entering the userid 5. If the assigned authentication scheme for the user is userid/password, then the user is prompted to enter his userid and password The identification and authentication to the IM component is accomplished via userid/password combination.
5	FIA_UAU.5	The MQAssure™ NetSignOn v3.0 component of the TOE have the following multiple authentication mechanisms. One of the following authentication mechanisms is used to log into the MQAssure™ NetSignOn v3.0 component: 1. userid and password 2. userid, MyKAD, and Biometrics 3. userid, MyKAD, and PIN / Password 4. userid, eKey USB Token, and PIN 5. userid, Iris Biometric Notice that userid must be entered prior to authenticating users via: 1. PIN / password of Biometric if MyKAD is used 2. PIN if eKey is used 3. Iris Biometric if Iris Authentication Schema is used 4. Password if userid and password combination is used Userid must be combined with either MyKAD or eKey or Iris or password authentication scheme in the evaluated configuration.
6	FIA_UAU.6	In the event that the users are logged out of their systems, the MQAssure™ NetSignOn v3.0 component requires them to re-authenticate themselves. The users must first press Ctrl-Alt-Del prior to the authentication to the domain using one of the following authentication mechanisms:

No.	SFR	Description
		1. userid and password 2. userid, MyKAD, and Biometrics 3. userid, MyKAD, and PIN / Password 4. userid, eKey USB Token, and PIN 5. userid and iris Biometric In the event that the users are locked or logged out of IM, they are required to re-authenticate themselves. The users must enter their userid's and passwords. Note that the locked out state is defined as when the users of IM has reached the maximum number of allowable login trials whether the authentication has failed. The logged out state is defined as when the users of IM or MQAssure™ NetSignOn v3.0 component choose to log out.

Table 15: TSS for Identification & Authentication

7.1.3 Security Management

No.	SFR	Description
1	FMT_MSA.1	The users are allowed to change their passwords through IM or MQAssure™ NetSignOn v3.0 User Application. They are 3 different reasons for users to change their passwords in IM: 1. Change at first time login to IM. 2. Unlock the user accounts or the users forgot the password (in IM or through MQAssure™ NetSignOn v3.0 User Application) 3. The users want to change their passwords.
2	FMT_MSA.3	The default PIN / password (for either userid or MyKAD authentication scheme) are the same as the assigned userid. The users can change their passwords using IM or MQAssure™ NetSignOn v3.0 User Application. The new passwords must adhere to the password quality as defined above in FIA_SOS.1.
3	FMT_SMF.1	The TOE users can change their: 1. Passwords for userid authentication scheme (using IM or MQAssure™ NetSignOn v3.0 User Application) 2. PINs / password for MyKAD authentication scheme (using IM or MQAssure™ NetSignOn v3.0 User Application) The reasons for changes are specified above in FMT_MSA.1
4	FMT_SMR.1	The users' roles are maintained by the TOE to determine what the users can access. TOE identified 2 roles, which is administrator and user role. If user authenticates as role "user" in IAM, the user will get several functionalities such as access to user profile and viewing audit events logs. However, the user profile management functions

No.	SFR	Description
		(except changing password) and viewing audit events logs are not part of the scope. If user authenticates as role "administrator" in IAM, the user will get all TOE administrative functionalities. However, the role administrator and all administrative functionalities is not part of the scope. If user authenticates as role "user" or "administrator" in MQAssure™ NetSignOn v3.0, the user will get access into Windows and have privileges as assigned in Active Directory. However, the privilege as assigned in Active Directory is not part of the scope.

Table 16: TSS for Security Management