MQAssure™ NetSignOn Secure Desktop Login

EAL 1 Security Target

Version 1.7

Date: 08 February 2012

MAGNAQUEST SOLUTIONS SDN. BHD.

Document History

Version No.	Date	Revision Description
1.0	31 July 2010	First initial release to evaluator
1.1	11 August 2010	Reviewed and revised the logical scope of the TOE. Revised the SFR's based on comments from the evaluator. Added Security Audit SFR's.
1.2	15 October 2010	Reviewed and revised the SFR's based on comments from the evaluator.
1.3	02 November 2010	Reviewed and revised logical scope, SFR's and TSS sections based on comments from evaluator.
1.4	11 November 2010	Revised the MyKAD reader in section 2.2.2 based on the comments from evaluator.
1.5	19 November 2010	Revised the logical scope, security objective for the operational environment, and TSS based on comments from evaluator.
1.6	01 December 2010	Revised the IAM software to reflect the actual name of the software, and the combination of the authentication scheme required.
1.7	08February 2012	Modified a sentence of ST Section 2.3 (1(b))

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 Windows operating systems that provides secure authentication and interactive logon service
GUI	Graphical User Interface
NetSignOn	MQAssure™ NetSignOn Secure Desktop Login
IAM	MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™ IAM v1.0_CR6 (may also be refered to as MQAssure™ IAM 1.0)
iKey	iKey is a USB token that is used for a two-factor authentication
IM	MQAssure™ Identity Manager
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

Acronym	Meaning
LAN	Local Area Network
MB	Mega bytes
MHz	Mega Hertz
MyKAD	MyKAD is the official compulsory smart identity card of Malaysia. It contains a smart card chip.
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

1.3 References

- Common Criteria Part 1 Version 3.1 Revision 3
- Common Criteria Part 2 Version 3.1 Revision 3
- Common Criteria Part 3 Version 3.1 Revision 3
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 3

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 by the 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™ NetSignOn Secure Desktop Login
ST Version	Version 1.7
ST Publication Date	08 February 2012
TOE Identification	NetSignOn
TOE Version	Version 2.0
CC Identification	CC Version 3.1 Revision 3
Assurance Level	EAL 1
ST Author	Ros Yusoff
Keywords	NetSignOn

Table 2: TOE Reference

2.2 TOE Overview

MQAssure™ NetSignOn 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, USB token, and userid/password to perform the login functionality to a system in a Domain (Network connected mode and network disconnected mode).

NetSignOn 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

NetSignOn is a client agent that runs on Windows operating systems. The TOE only covers NetSignOn 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, iKey 2032 with 32KB (iKey) 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)
2	Operating System / Software	• For NSO client ▪ Windows XP (32 bit or 64 bit) ▪ Windows Vista (32 bit or 64 bit) ▪ Windows 7 (32 bit or 64 bit) ▪ Also, requires the following software: • CID308 reader driver (for using MyKAD) • iKey smart card reader driver (for using iKey) • Internet Explorer 8.0 (for accessing IAM web application) • For IAM Server ▪ Windows 2003 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 8.0 (for accessing IAM web application) • For Directory Server ▪ Windows 2003 Enterprise Edition with service pack 2 or above ▪ Also, requires the following software; • Active Directory (LDAP compliant)
	Hardware	• For NSO 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 iKey is to be used as the authentication token) ▪ CID308 MyKAD reader (if MyKAD is to be used as the authentication token) ▪ Biometric reader with Sagem finger print sensor (if finger print is to be used along with MyKAD) • 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

No.	Requirement	Version / Specification
		▪ 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

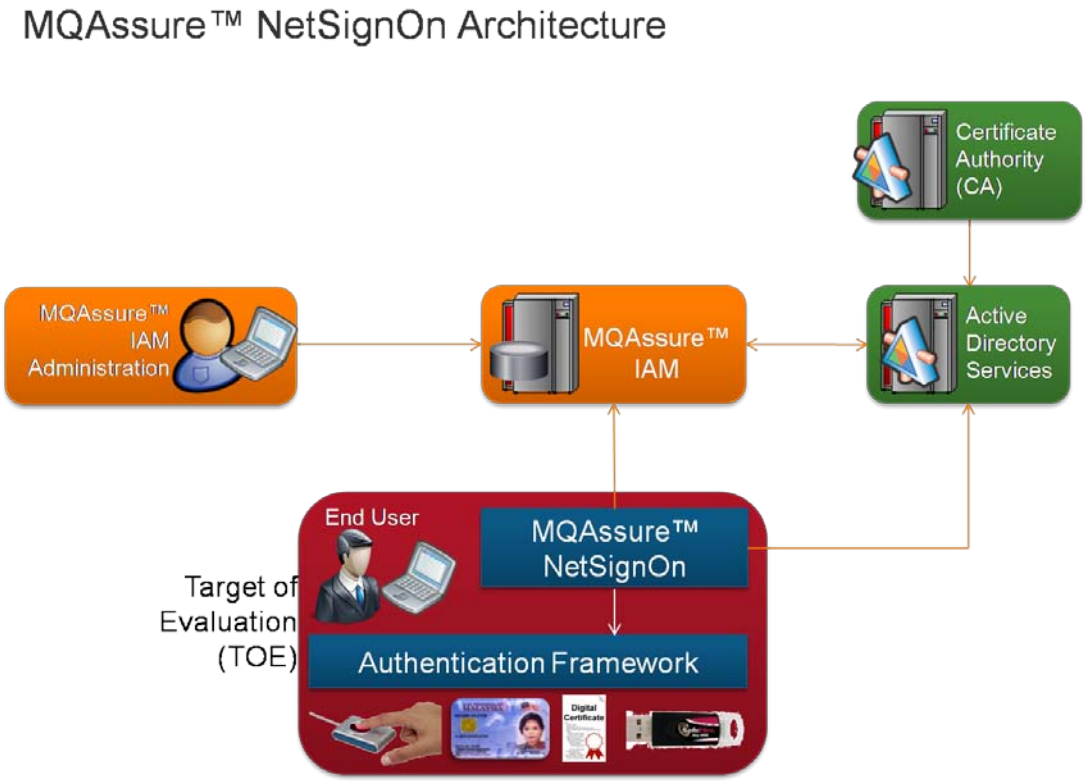

Figure 1: NetSignOn Architecture

Figure 1 depicts the architecture of NetSignOn. It has the following components.

1. MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™ IAM v1.0_CR6 (MQAssure™ IAM 1.0 or IAM)

IAM is a centralized identity and access management platform. It provides the backbone for the NetSignOn by providing centralized policy management (part of IM), session management and audit logging (part of AM). In the overall infrastructure NetSignOn 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 enforcing the authentication policy and reports viewing function which is within the scope of the TOE. Additionally, only Self-help function for TOE users is within the scope of the 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.

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. NSO

NetSignOn is implemented as a custom GINA dll in Windows. This provides the login interface to the users to login to their respective workstations. NetSignOn makes use of the MQAssure™ IAM 1.0 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 iKey serial number, MyKAD number, PIN / password for MyKAD, and passwords. PIN for the iKey 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;

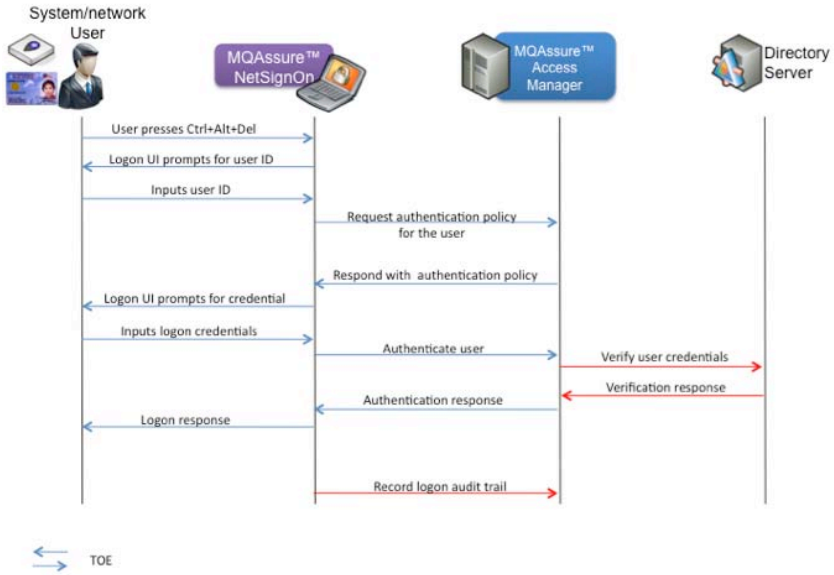

Figure 2: NetSignOn Process

Note from the above figure (Figure 2) that:

1. The TOE is only for the usage of NSO 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. iKey/PIN: Users can login to the system / network by inserting their iKey into the USB reader and then type in their PIN

The following management functions are not part of the TOE:

1. Registration or enrollment of users into IAM
2. Enrollment of user credentials into MyKAD or iKey
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. Self-help function in IM for the administrator of IAM and NSO

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 combination, or MyKAD and Biometric (finger printing) combination, or iKey and PIN combination. Userid and password combination must be combined with either MyKAD or iKey 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 NSO component choose to log out.
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 iKey or MyKAD), 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 disabled 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. 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 for MyKAD can be changed using IM. The second type, which is the PIN for iKey, can be changed via the iKey software itself since it's stored in the iKey itself. iKey and its related software are not part of the TOE. User accounts are disabled after a number of unsuccessful authentication attempts (default is 3 attempts) in IM. And, users must be re-authenticated once they are either locked or logged out of the domain.

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.3 conformant**. The TOE and ST are Common Criteria conformant to Common Criteria version 3.1 Revision 3.
- **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) 1.
- The TOE and ST does not conform to **Protection Profiles**.

4 SECURITY OBJECTIVES

4.1 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 iKey) 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.
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 5: Security Objective for the Operational Environment

5 SECURITY REQUIREMENTS

This section specifies the requirements for the TOE.

5.1 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 initialisation
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security Roles

Table 6: TOE Security Functional Requirements

5.1.1 User Data Protection

5.1.1.1 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 NetSignOn by performing the run-time check at the IAM level].

5.1.1.2 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 iKey
    v. Serial number for iKey
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 iKey and PIN, then the user is prompted to insert his iKey into the USB port and provide the PIN
d) 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].

5.1.2 Identification and Authentication

5.1.2.1 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 [*an administrative configurable positive integer within 1 to 99*] unsuccessful authentication attempts occur related to [authentication page in IM].

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

5.1.2.2 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 iKey
    v. Serial number for iKey
d) Role].

5.1.2.3 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 iKey.*

5.1.2.4 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.*

5.1.2.5 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 NSO component in the form of:

a) userid and password
b) userid, MyKAD, and Biometrics
c) userid, MyKAD, and PIN / Password
d) userid, iKey USB Token, and PIN]

to support user authentication.

FIA_UAU.5.2: The TSF shall authenticate any user's claimed identity according to the [authentication policy of the NSO 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 iKey and PIN, then the user is prompted to insert his iKey into the USB port and provide the PIN
d) If the assigned authentication scheme for the user is userid and password, then the user is prompted to enter his password].

5.1.2.6 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].

5.1.2.7 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

5.1.3 Security Management

5.1.3.1 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*] the security attributes [password for userid, and PIN / password for MyKAD] to [TOE users].

Application Note: *The users can change the PIN / passwords in IM for userid or MyKAD authentication scheme.*

5.1.3.2 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.

5.1.3.3 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].

5.1.3.4 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.*

5.2 TOE Security Assurance Requirement

The TOE meets the security assurance requirements for EAL1. The following table is the summary for the requirements:

Assurance Class	Assurance Components
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance AGD_PRE.1 Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1 Labeling of the TOE ALC_CMS.1 TOE CM Coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.1 Security objectives for the operational environment ASE_REQ.1 Stated security requirements ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independence Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

Table 7: TOE Security Assurance Requirements

6 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.

6.1 TOE Security Functions

6.1.1 User Data Protection

No.	SFR	Description
1	FDP_ACC.1	NSO 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. This authentication scheme is only supported at the NSO component (not applicable when user login to IAM). The management of the scheme is however performed at the IAM component. 3. Userid, MyKAD and Biometric (finger printing) combination 4. Userid, iKey and PIN 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.
2	FDP_ACF.1	The access control policy 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. Biometric reference for MyKAD iv. PIN for iKey v. Serial number for iKey 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 Biometric, then the user is prompted to insert his MyKAD into the reader and place the thumb on the finger print scanner.

No.	SFR	Description
		If the assigned authentication scheme for the user is iKey and PIN, then the user is prompted to insert his iKey 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 8: TSS for User Data Protection

6.1.2 Identification and Authentication

No.	SFR	Description
1	FIA_AFL.1	The user accounts are disabled after a defined number of unsuccessful authentication attempts when users log in to IM (not in the NSO component). 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. PIN for iKey v. Serial number for iKey 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 is only relevant for the PIN / password for userid and MyKAD. 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 process is not part of the TOE).
4	FIA_UAU.2 & FIA_UID.2	Users can only access the TOE (NSO component and IM component for password management) once they are identified and authenticated. The identification and authentication to the NSO component is

No.	SFR	Description
		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 iKey/PIN, then the user is prompted to insert his iKey into the USB port and provide the PIN after entering the userid 4. 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 NSO component of the TOE have the following multiple authentication mechanisms. One of the following authentication mechanisms is used to log into the NSO component: 1. userid and password 2. userid, MyKAD, and Biometrics 3. userid, MyKAD, and PIN / Password 4. userid, iKey USB Token, and PIN Notice that userid must be entered prior to authenticating users via: 1. PIN / password of Biometric if MyKAD is used 2. PIN if iKey is used 3. Password if userid and password combination is used Userid and password combination must be combined with either MyKAD or iKey authentication scheme in the evaluated configuration.
6	FIA_UAU.6	In the event that the users are logged out of their systems, the NSO 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: 1. userid and password 2. userid, MyKAD, and Biometrics 3. userid, MyKAD, and PIN / Password 4. userid, iKey USB Token, and PIN 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 NSO component choose to log out.

Table 9: TSS for Identification & Authentication

6.1.3 Security Management

No.	SFR	Description
1	FMT_MSA.1	The users are allowed to change their passwords through IM. 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) 3. The users want to change their passwords in IM
2	FMT_MSA.3	The default PIN / password (for either userid or myKAD authentication scheme) is the same as the assigned userid. The users can change their passwords using IM. 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) 2. PINs / password for MyKAD authentication scheme (using IM) 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 (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 NSO, 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 10: TSS for Security Management