MQAssure™/AppShield v1.2 integrated with MQAssure™/IAM v1.0

Security Target

Version 1.21

03 January, 2011

Prepared for

MagnaQuest Solutions Sdn Bhd

A-2-07 & A-2-09

SME Technopreneur Centre Cyberjaya

2270, Jalan Usahawan 2

63000, Cyberjaya, Selangor DE, Malaysia

www.magnaquest.com

Revision History

Version	Date (DD/MM/YYYY)	Written By	Checked By	Changes
1.21	03/01/2011	Binumon T K	Shince Thomas	Final Release

Trade marks

"MQAssure™" is a trademark of MagnaQuest Solutions Sdn Bhd

Company Titles

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

MagnaQuest Solutions Sdn Bhd - 'MagnaQuest'

Document Titles

The following title referred as the latest TOE version and used for all documents in TOE evaluations.

"MQAssure™/AppShield v1.2 integrated with MQAssure™/IAM v1.0**"**

Table of Contents

Tables

Figures

1. Introduction

This introductory section presents security target (ST) identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided

1.1 ST and TOE Identification

1.1.1 ST Reference

Item	Reference
ST Title	Security Target for the MQAssure™/AppShield v1.2 Integrated with MQAssure™/IAM v1.0
ST Date	03/01/2011
ST Version	1.21

Table 1- ST Reference

1.1.2 TOE Reference

Item	Reference
TOE Name and Version	MQAssure™/AppShield v1.2_CR6 Integrated with MQAssure™/IAM v1.0_CR6

Table 2- TOE Identifiers

1.2 TOE Overview

MQAssure™/AppShield (AppShield) integrated with MQAssure™/IAM (IAM) provides security to web applications by enforcing authentication and authorization. It readily augments multifactor authentication capability to the web applications without modifying application code. AppShield software is a self contained product with built in User and Access management. In the latest upgrade as stated in Table 2, AppShield has undergone architectural changes mainly involving separation of the management functionality from the enforcement. The administration and management aspects of AppShield have been moved to IAM. The enforcement of authentication and authorization policies is done by the AppShield. Hence the TOE covers both the AppShield and IAM.

AppShield is able to shield web applications from a number of common input tampering attacks by scanning all the input parameters and validate the requests against the rules defined for the web application.

IAM is a centralized identity and access management platform. It provides the back bone for the AppShield by providing centralized policy management, session management and audit logging. In the overall infrastructure AppShield acts as a policy enforcement agent for web applications. IAM provides a centralized administration console through which the administrators can create and enforce various policies to control the access to various web application resources protected by AppShield.

IAM supports various authentication schemes such as User name/password, smartcard, biometric and USB token which is leveraged by AppShield to enforce multifactor authentication for web applications. The TOE can also support credentials from smartcard reader of Smartek CID from Integrity. It also can support SafeNet iKey USB tokens.

The MQAssure™ client (Client) provides a browser plug-in that communicates to the tokens and devices to retrieve the user credentials. The role of the client is simply as a mechanism to assist the entry of authentication credentials. The client is not part of the TOE.

The product can be configured to provide alerts on various user defined security events. These alerts can be delivered to respective application users and security administrators through email. The security administrator can define the alert events against each application.

The TOE provides privileges for administrators to provision users, assign role and authentication schemes to user, manage policies and monitor various server runtime parameters. The web based console provided by the TOE can be used for the administration and configuration of the TOE.

The TOE also provides various audit reports based on security events such as failed user login and password resets. Printing of these audit reports supports various document formats like MS Word document and PDF.

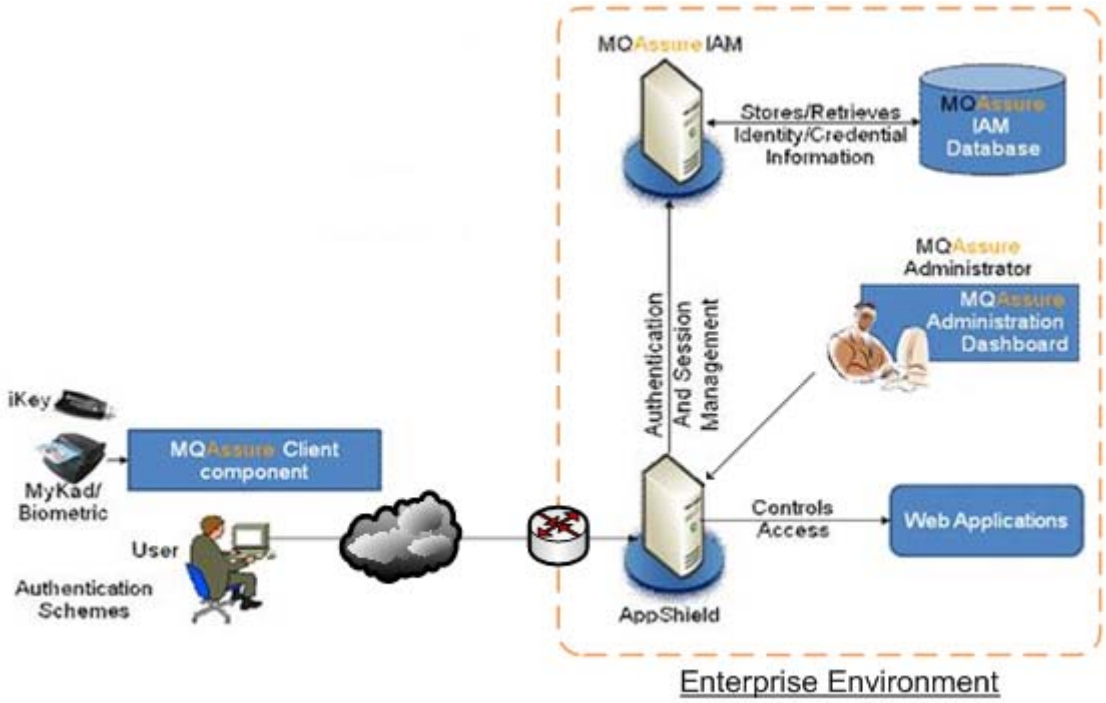

Figure 1 - TOE Operating Environment

NOTE: MQAssure™/IAM Database is a part of the TOE environment and thus not in the scope of TOE evaluation

1.2.1 Required Firmware/Hardware/Software

The TOE requires a range of hardware and software in order to install the TOE and support the security functionality. This is provided in Table 3 below

Item	Description	Scope
Hardware	Server Hardware - A standard workstation or server class machine with 2.4 GHz or higher Intel processor, 2 GB or more RAM, running Windows 2003 Server Client Hardware - A standard workstation or laptop with 1.6 GHz or higher Intel/AMD processor, 1 GB or more RAM, running Windows XP or Vista or	Environment

	2003 Server - E-ID Smart Card (For evaluation purpose, Malaysian Identity Card (MyKAD) is used) - E-ID Smart Card reader (For evaluation purpose, Smartec CID 308 is used. The reader must be PC/SC compliant) - USB token (For evaluation purpose, SafeNet iKey 2032 is used)	
Software	Application Server - GlassFish 2.1 - Tomcat Server 5.5.9	Environment
	Database Server - MySQL 5.0	Environment
	Mail Server - SMTP Server - POP3 Server	Environment
	Browser - IE v6.0 to IE v8.0	Environment
	Client Component - Smartec CID Drivers (Not applicable if user not using MyKad/Biometric Scheme) - SafeNet iKey 2032 Drivers (Not applicable if user not using iKey/PIN Scheme) - MQAssure™ Client Components version CR3 (Not applicable if user only use Password Scheme) - IE v6.0 to IE v8.0	Environment
Firmware	Specific to the Hardware.	Environment

Table 3 - Required Firmware/Hardware/Software

1.3 TOE Description

This section provides context for the TOE evaluation.

AppShield enforces authentication and authorization for accessing the web applications, leveraging the authentication schemes supported by IAM. IAM accepts MyKad/Biometric, iKey/PIN and User name/password authentication schemes. AppShield can enforce role and policy based access control on business functionality. This is done in conjunction with the IAM policy manager. Thus AppShield helps web applications to delegate authentication and authorization functionalities thus enabling the applications to remain insulated from the changing security demands of the organizations. AppShield also provides an additional insulation layer by filtering HTTP parameters.

IAM supports various kinds of security policies for authorization like location-based (IP Address), strong password and password expiry which are enforced by AppShield. The IAM session manager performs various session management activities like session timeout and forced logoff. AppShield validates the session through the IAM session manager each time an access request comes to the web application.

IAM provides a web based console for the administration and configuration. Through this console, the administrator would be able to perform User provisioning, assigning roles and authentication schemes for Users, managing policies and monitoring various runtime details for example monitoring user session.

The Audit & Alerts Service ensures that all the security events that were defined as critical at the time of application security configuration will be logged and audit reports are generated against these events. The solution also supports delivery of alerts on critical security events through email.

1.3.1 Scope of the TOE

The TOE is a software product, which comprises of MQAssure™/AppShield v1.2 Integrated with MQAssure™/IAM v1.0.

All underlying supporting hardware and software of both IAM and AppShield are not considered part of the TOE, including the IAM database. Web applications protected by AppShield are also part of the environment.

As the client (authentication component) is considered a mechanism to assist the entry of authentication credentials, it is not considered part of the TOE.

Figure 2 demonstrates the scope of the TOE.

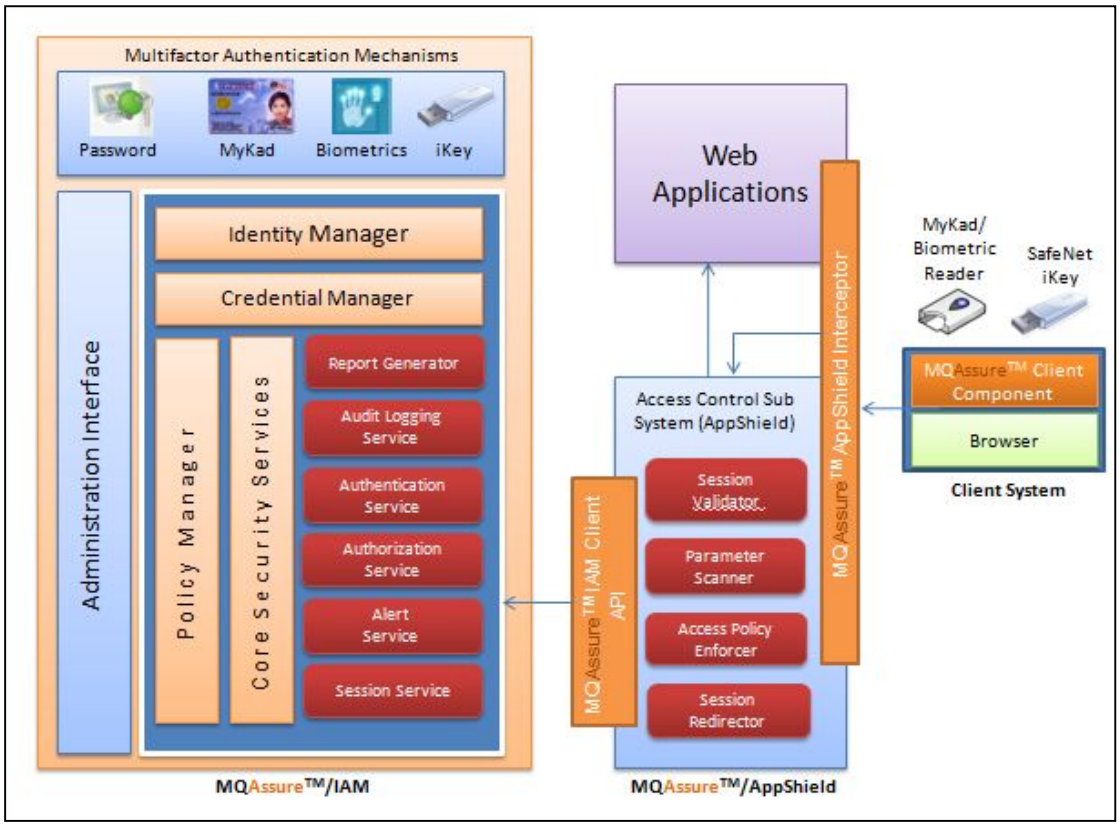

Figure 2: TOE Architecture

The Security features provided by the TOE (IAM and AppShield) are provided in Table 4 and Table 5 below.

Item	Description
Strong Multifactor User Authentication	The TOE accepts multiple authentication schemes including: • MyKad/Biometric • iKey/PIN • Password
TOE Administration	The TOE provides a web based GUI console for the administrator to configure and manage the TOE. The TOE provides the following management capability: • Identity management • Session Services • Policy management

	• Audit reporting
Security Audit	The TOE generates audit records for relevant authentication events such as Login, Logout, Login failure, logout failure, account locks and access events such as creation, modification, deletion, approval and denial of various objects.

Table 4 - Security features of MQAssure™/IAM

Item	Description
Access Control	AppShield enforces access control policy decisions made by the IAM server. The access control decisions are made based on User role, requested resource and requested operations. The policy management component of IAM allows the administrator to define various access control policies
HTTP request validation	AppShield is able to shield web applications from a number of common input tampering attacks by scanning the input parameters and validate the requests against the rules defined for the web application.

Table 5 - Security features of MQAssure™/AppShield

2. Conformance Claims

2.1 Claims

Item	Conformance Claim
Applicable Criteria	- Common Criteria (CC) version 3.1 Revision 3 Part 2 Conformant - Common Criteria (CC) version 3.1 Revision 3 Part 3 Conformant
Protection Profiles	This ST does not claim conformance to any Protection Profiles
Security Assurance Package	EAL4 security assurance package defined in Common Criteria (CC) version 3.1 revision 3 Part 3. This ST is EAL4 conformant

Table 6 - Conformance Claims

3. Security Problem Definition

3.1 Threats

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

Identifiers	Description
T.WEAK_PASS	A user may select a weak password thereby enabling an attacker to access restricted web applications compromising the confidentiality of enterprise data.
T.DATA_ACCESS	An unauthorized person views restricted hosted content compromising the confidentiality and integrity of enterprise data.
T.WEB_ATTACK	An attacker may compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.
T.USER_PARAM	A user may inadvertently compromise the integrity and availability of enterprise data protected by the TOE by inserting potentially dangerous input into insecure web applications.
T.RECONFIG	An Attacker attempts to reconfigure the TOE to gain access to protected enterprise data compromising integrity and confidentiality.

Table 7 - Threats addressed by the TOE

3.2 Security Assumptions

The following assumptions, listed in Table 8 below, relate to the operation of the TOE.

Identifiers	Description
A.NO_EVIL	TOE Administrators and TOE users are assumed to be non-hostile and trusted to perform all their duties in a competent manner
A.PHYS_SEC	IAM and AppShield will be hosted inside of a physically secure area.

A.TIME_STAMP	The environment will provide reliable time stamps to the TOE.
A.MAIL_SERVER	The environment will provide a mail server to facilitate alerts from TOE in the form of email.
A.IAM_PROTECT	The environment is configured to block all traffic to the IAM server except for traffic required to perform security functionality.
A.TRANS_PROTECT	The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and AppShield server.
A.IAM_DATA	The IAM database is located within the enterprises network boundary and is configured so that only TOE administrators can directly access the interface of the database.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS traffic to pass through to AppShield.

Table 8 – Assumptions

4. Security Objectives

4.1 Objectives for the Operational Environment

The security objectives for the TOE environment are those specified in Table 9 below.

Identifiers	Description
OE.NO_EVIL	TOE Administrators and TOE users shall not be hostile and trusted to perform all their duties in a competent manner
OE.PHYS_SEC	The Enterprise Administrator shall ensure that the IAM and AppShield servers are hosted inside of a physically secure area.
OE.TIME_STAMP	The environment shall provide reliable time stamps to the TOE.
OE.MAIL_SERVER	The Enterprise Administrator shall ensure that a mail server is available to facilitate email alerts from TOE.
OE.IAM_PROTECT	The IAM environment is configured to block all traffic to the IAM server except for traffic required to perform security functionality.
OE.TRANS_PROTECT	The IT environment shall provide the server-side of a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and AppShield server.
OE.IAM_DATA	The Enterprise Administrator shall ensure that the IAM database is located within the enterprises network boundary and is configured so that only TOE administrators can directly access the interface of the database.
OE.FIREWALL	The Enterprise Administrator shall ensure that gateway filtering is implemented; only allowing HTTP and HTTPS traffic to pass through to AppShield.

Table 9 – Security objectives of the environment

4.2 TOE Security Objectives

The security objectives for the TOE are described in below in Table 11.

Identifiers	Description
O.ACC_CONTROL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
O.LOCKOUT	The TOE shall disable accounts after an administratively defined amount of failed logins.
O.RESTRICT_AUTH	The TOE shall be able to restrict access to protected applications based on login time and assumed IP address.
O.AUTH_MECH	The TOE shall accept multiple authentication mechanisms to strengthen user authentication.
O.AUDIT	The TOE shall generate audit reports to trace User and administrator access events
O.SECURE_CONFIG	The TOE shall ensure that only administrator role can perform the configuration changes in the TOE and enrolment of new Users.
O.ALERT	The TOE shall provide alert mechanism through email to notify assigned Users on the access control violations
O.FILTER	The TOE shall filter HTTP requests to prevent common input tampering attacks by scanning all the input parameters and validate the requests against the rules defined for the web application.

Table 10 – Security objectives of the TOE

4.3 Security Objectives Rationale

4.3.1 Security objectives for the TOE

SPD Component	Objective	Justification
T.WEAK_PASS	O.LOCKOUT O.ALERT O.AUDIT O.AUTH_MECH	The threat of a user selecting a weak password resulting in an attacker gaining access is mitigated by: • O.LOCKOUT - The TOE will greatly reduce the chance of

		guessing passwords by reducing the number of possible attempts. Brute force attacks are also rendered ineffective. • O.AUTH_MECH - The TOE can be configured to accept stronger means of authentication such as non-forgeable biometrics. Additionally, complex passwords can be enabled to block weak passwords. • O.AUDIT - All login attempts (successful or unsuccessful) will be logged. • O.ALERT - The TOE shall provide alert mechanism through email to notify assigned Users on the access control violations
T.DATA_ACCESS	O.ACC_CONTROL O.AUTH_MECH O.RESTRICT_AUTH O.AUDIT	The threat of an attacker gaining access to restricted content is mitigated by: • O.ACC_CONTROL - The TOE shall ensure that only authenticated and authorized Users can access the TOE functionality and protected application resources. • O.RESTRICT_AUTH - The TOE shall be able to restrict access to protected applications based on login assumed IP address. • O.AUTH_MECH - The TOE shall accept multiple authentication mechanisms providing the enterprise with the option to choose the mechanism that best fits the threat environment. • O.AUDIT - The TOE shall generate audit reports to trace User and administrator access

		events
T.WEB_ATTACK	O.FILTER O.ACC_CONTROL	The threat of web application attacks is mitigated by: • O.FILTER - The TOE shall filter HTTP requests to prevent common input tampering attacks by scanning all the input parameters and validate the requests against the rules defined for the web application. • O.ACC_CONTROL - The TOE shall ensure that only authenticated and authorized Users can access the TOE functionality and protected application resources.
T.USER_PARAM	O.FILTER	The threat of a user accidently inserting potentially dangerous input into insecure web applications is mitigated by: • O.FILTER - The TOE shall filter HTTP requests to prevent common input tampering attacks by scanning all the input parameters and validate the requests against the rules defined for the web application.
T.RECONFIG	O.SECURE_CONFIG	The threat of unauthorized configuration is mitigated by: • O.SECURE_CONFIG - only the administrator role can perform configuration changes in the TOE and enrolment of new Users.

Table 11 - Mapping of threats to the security objectives of the TOE

4.3.2 Security objectives for the Environment

SPD Component	Objective	Justification
A.NO_EVIL	OE.NO_EVIL	This objective for the environment ensures that the assumption is upheld that TOE administrators and users are trusted and will perform their duties correctly.
A.PHYS_SEC	OE.PHYS_SEC	This objective for the environment ensures that the assumption is upheld that the IAM and AppShield servers are hosted inside of a physically secure area.
A.TIME_STAMP	OE.TIME_STAMP	This objective for the environment ensures that the assumption is upheld that the environment will provide reliable time stamps.
A.MAIL_SERVER	OE.MAIL_SERVER	This objective for the environment ensures that the assumption is upheld that the environment will provide a mail server to the TOE.
A.IAM_PROTECT	OE.IAM_PROTECT	This objective for the environment ensures that the assumption is upheld that the IAM Server is located within the enterprise network boundary and is protected from unauthorized physical access. Additionally, the environment is configured to block all traffic to the IAM server except for traffic required to perform security functionality.
A.TRANS_PROTECT	OE.TRANS_PROTECT	This objective for the environment ensures that the assumption is upheld that the environment will provide a method for secure transmission of information (and credential) from the user to AppShield.

A.IAM_DATA	OE.IAM_DATA	This objective for the environment ensures that the assumption is upheld that access to the IAM database is restricted to TOE administrators.
A.FIREWALL	OE.FIREWALL	This objective for the environment ensures that the assumption is upheld that gateway filtering is implemented; only allowing HTTP and HTTPS traffic to pass through to AppShield.

Table 12 - Mapping of assumptions to security objectives for the environment

5. Security Requirements

5.1 SFR formatting

The following conventions are set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.

5.1.1 The refinement operation is used to add or remove detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text** for additional details and ~~**strike through underline text**~~ for removing detail of a requirement.

5.1.2 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*].

5.1.3 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].

5.1.4 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).

5.2 Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in Table 13, below.

No	Component	Component Name
Class FAU: Audit		
1.	FAU_SAA.1	Potential violation analysis

2.	FAU_ARP.1	Security alarms
3.	FAU_GEN.1	Audit data generation
4.	FAU_GEN.2	User identity association
5.	FAU_SAR.1	Audit review
6.	FAU_SAR.2	Restricted audit review
Class FDP: User data protection		
7.	FDP_ACC.1	Subset access control
8.	FDP_ACF.1	Security attribute based access control
Class FIA: Identification and Authentication		
9.	FIA_AFL.1	Authentication failure handling
10.	FIA_ATD.1	User attribute definition
11.	FIA_SOS.1	Verification of secrets
12.	FIA_UAU.2	User authentication before any action
13.	FIA_UAU.5	Multiple authentication mechanisms
14.	FIA_UAU.6	Re-authenticating
15.	FIA_UID.2	User identification before any action
Class FMT: Security management		
16.	FMT_MSA.1	Management of security attributes
17.	FMT_MSA.3	Static attribute initialization
18.	FMT_SMF.1	Specification of management functions
19.	FMT_SMR.1	Security roles
20.	FMT_SAE.1	Time-limited authorisation
Class FTA : TOE access		
21.	FTA_MCS.1	Basic limitation on multiple concurrent sessions
22.	FTA_SSL.3	TSF-initiated termination

23.	FTA_TAH.1	TOE access history
24.	FTA_TSE.1	TOE session establishment

Table 13 - TOE Security Functional Requirements (SFRs)

5.2.1 Security audit (FAU)

5.2.1.1 Potential violation analysis (FAU_SAA.1)

Hierarchical to: No other components.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

- Accumulation or combination of [repeated logon failure, repeated unsuccessful access requests] known to indicate a potential security violation
- [None]

Dependencies: FAU_GEN.1 Audit data generation

5.2.1.2 Security Alarms (FAU_ARP.1)

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [email an alert message to administrator] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

5.2.1.3 Audit data generation (FAU_GEN.1)

Hierarchical to: No other components.

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

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

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

c) [

	Addition or removal of application resources in the TOE; Success or failure of User authentication; All the operations (creation, deletion and modification) of the password policies; All the operations (creation, deletion and modification) of User profile All the operations (creation, deletion, activation and deactivation) of User Role;]
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [audit severity]
Dependencies	FPT_STM.1 Reliable time stamps (fulfilled by environment)

5.2.1.4 User identity association (FAU_GEN.2)

Hierarchical to:	No other components.
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

5.2.1.5 Audit review (FAU_SAR.1)

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [TOE Administrators] with the capability to read [a) Audit time stamp b) Audit details c) Subject of the audit event d) Audit severity] from the audit records.

FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies	FAU_GEN.1 Audit data generation

5.2.1.6 Restricted audit review (FAU_SAR.2)

Hierarchical to:	No other components.
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access
Dependencies	FAU_SAR.1 Audit review

5.2.2 User data protection (FDP)

5.2.2.1 Subset access control (FDP_ACC.1)

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [access control policies] on [Subjects (User and Role), Objects (Resource and Audit Logs) and Operations (Read, Write and Delete) covered by the SFP].
Dependencies	FDP_ACF.1 Security attribute based access control

5.2.2.2 Security attribute based access control (FDP_ACF.1)

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [access control policies] to objects based on the following: [Subject: Role – role name, business unit, permissions User – User name, password, iKey PIN, organization unit, role, location Objects: Resource – Resource Name, Resource ID, Resource IP, Resource Port Audit Log – Audit Log ID, Audit Time]
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 the user request to access a web resource (URL), the MQAssure™/AppShield authenticates the User if he/she does not have a valid logged-in session - After authenticating the User, the MQAssure™/AppShield passes the User Name, Role, Resource URL, Client Host IP and Current Time in an XACML request format, to the MQAssure™/IAM Policy Manager - MQAssure™/IAM Policy Manager evaluates the request attributes against the list of organizational policies and selects the matching policy. - The policy manager then sends the policy decision (Allow/Deny) and obligation (Audit/Not to Audit) as per the selected policy, to the MQAssure™/AppShield, in XACML format - The MQAssure™/AppShield denies the User access if the policy decision is to 'Deny' and forwards the User request to the web resource if the policy decision is 'Allow' - The MQAssure™/AppShield also acts on the policy obligation to audit the event].
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 [None]
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

5.2.3 Identification and Authentication (FIA)

5.2.3.1 Authentication failure handling (FIA_AFL.1)

Hierarchical to:	No other components.

FIA_AFL.1.1	The TSF shall detect when [*an administrator configurable positive integer within* [*3-9*]] unsuccessful authentication attempts occur related to [AppShield Authentication]s
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [disable the user account]
Dependencies	FIA_UAU.1 Timing of authentication

5.2.3.2 User attribute definition (FIA_ATD.1)

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [a) User Name b) Type of the authentication scheme assigned c) Credential for the assigned authentication scheme d) Role e) Authentication Failure counter f) status]
Dependencies	No dependencies

5.2.3.3 Verification of secrets (FIA_SOS.1)

Hierarchical to:	No other components
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [the following quality checks configured by the TOE Administrator for TOE User Authentication: a) include numeric characters; b) contain complex characters; c) not contain a repeating predictable sequence; and d) contain minimum number of characters].
Dependencies	No dependencies

5.2.3.4 User authentication before any action (FIA_UAU.2)

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.

Dependencies	FIA_UID.1 Timing of identification (fulfilled by FIA_UID.2)

5.2.3.5 Multiple authentication mechanisms (FIA_UAU.5)

Hierarchical to:	No other components.
FIA_UAU.5.1	The TSF shall provide [a mechanism to accept credentials in the form of MyKad, Biometric, iKey USB Token and Password] to support user authentication
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [authentication SFP such that: a) 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 over the finger print scanner and the AppShield performs a 1:1 match of the users live fingerprint minutiae against the stored fingerprint minutiae in the MyKad and then verifies the MyKad details with the MQAssure™ IAM server b) If the assigned authentication scheme for the user is iKey/PIN then the AppShield prompts the user to insert the iKey into the USB port of his PC and enter the PIN to unlock the iKey. If the PIN entered is right then the AppShield will be able to unlock the iKey. AppShield will verify whether the iKey serial number inserted is the same with iKey serial number registered for that particular user with MQAssure™ /IAM server. c) If the assigned authentication scheme for the user is user ID and password then the AppShield prompts the user to enter his user ID and password and then sends the password hash to the MQAssure™/IAM server for verification]
Dependencies	No dependencies.

5.2.3.6 Re-authenticating (FIA_UAU.6)

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [a) Session timeout]
Dependencies	No dependencies.

5.2.3.7 User identification before any action (FIA_UID.2)

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies	No dependencies

5.2.4 Security management (FMT)

5.2.4.1 Management of security attributes (FMT_MSA.1)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [access control policy] to restrict the ability to [*change default, modify, delete,* [*create*]] the security attributes [role and access privileges of Users] to [TOE administrators].
Dependencies	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

5.2.4.2 Static attribute initialization (FMT_MSA.3)

Hierarchical to:	No other components.
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 administrators] to specify alternative initial values to override the default values when an object or information is created.
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

5.2.4.3 Specification of management functions (FMT_SMF.1)

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [a) Identity management b) Audit reporting c) Policy management d) Session Services

].

Dependencies	No dependencies

5.2.4.4 Security roles (FMT_SMR.1)

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles: [User, Administrator and Approver].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies	FIA_UID.1 Timing of identification (fulfilled by FIA_UID.2)

5.2.4.5 Time-limited authorisation (FMT_SAE.1)

Hierarchical to:	No other components.
FMT_SAE.1.1	The TSF shall restrict the capability to specify an expiration time for [password] to [TOE Administrators].
FMT_SAE.1.2	For each of these security attributes, the TSF shall be able to [disable the user account] after the expiration time for the indicated security attribute has passed.
Dependencies	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps (fulfilled by environment)

5.2.5 TOE access (FTA)

5.2.5.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

Hierarchical to:	No other components.
FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of [1] sessions per user
Dependencies	FIA_UID.1 Timing of identification (fulfilled by FIA_UID.2)

5.2.5.2 TSF-initiated termination (FTA_SSL.3)

Hierarchical to:	No other components.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [an administratively configurable amount of time of user inactivity]
Dependencies	No dependencies

5.2.5.3 TOE Access History (FTA_TAH.1)

Hierarchical to:	No other components.
FTA_TAH.1.1	Upon successful session establishment, the TSF shall display the [*date, time, method and location*] of the last successful session establishment to the user
FTA_TAH.1.2	Upon successful session establishment, the TSF shall display the [*date, time, method and location*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment
FTA_TAH.1.3	The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information
Dependencies	No dependencies

5.2.5.4 TOE session establishment (FTA_TSE.1)

Hierarchical to:	No other components.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [IP address and HTTP request parameters].
Dependencies	No dependencies

5.3 Security Requirements Rationale

Objectives	SFR	Rationale
O.RESTRICT_AUTH	FTA_TSE.1	O.RESTRICT_AUTH is fulfilled in the following manner - FTA_TSE.1 will restrict sessions based on IP Address and HTTP request parameters.
O.ACC_CONTROL	FDP_ACC.1 FDP_ACF.1 FTA_SSL.3 FTA_MCS.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.6	O.ACC_CONTROL is fulfilled in the following manner - FDP_ACC.1 enforces access control policies when a subject controlled by the TOE accesses an object controlled by TOE to perform an operation - FDP_ACF.1 enforces the access control policies based on the user name and role attributes of the subjects and resource name, resource IP and operation attributes of the objects - FTA_SSL.3 terminates the user sessions after the session timeout - FTA MCS.1 restrict the number of concurrent sessions of the same user and by default it allows only1 session per user - FIA_UID.2 prevents user from performing any actions before getting successfully identified - FIA_UAU.2 prevents user from performing any actions before getting successfully authenticated - FIA_UAU.6 re-authenticates the user in the case of session timeouts
O.AUDIT	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2	O.AUDIT is fulfilled in the following manner - FAU_GEN.1 generates the required audit data - FAU_GEN.2 associates each auditable event with the identity of

	FAU_ARP.1 FAU_SAA.1 FTA_TAH.1	the user that caused the event. - FAU_SAR.1 allow only TOE administrators to read the audit data and the audit reports are presented in HTML or PDF formats - FAU_SAR.2 denies the audit data access to all the users except those who have been granted the read access - FAU_ARP.1 generates email based alerts as configured in the TOE for reporting access control violations - FAU_SAA.1 detect potential violation of the enforcement by applying set of rules in the recorded audit events - FTA_TAH.1 tracks the last successful session establishment by the user. Upon successful session establishment, the TOE displays the date, time, method and location of the last successful and un successful session establishment for his review
O.ALERT	FAU_ARP.1	O.ALERT is fulfilled in the following manner - FAU_ARP.1 generates email based alerts as configured in the TOE for reporting access control violations
O.SECURE_CONFIG	FMT_SMF.1 FMT_SMR.1 FMT_MSA.1 FMT_MSA.3 FMT_SAE.1	O.SECURE_CONFIG is fulfilled in the following manner - FMT_SMF.1 provides the management functions to manage user profiles, roles, policies and authentication schemes. It also provides functions to assign roles and authentication schemes to users. - FMT_SMR.1 maintains the roles and help to associate user with roles - FMT_MSA.1 shall enforce to restrict the ability to change default, create, modify and delete the security attributes (role and privileges of

		users) to TOE administrators - FMT_MSA.3 restrict the ability to provide the default values to security attributes to TOE administrators - FMT _SAE.1 allows only TOE administrators to configure the expiry time for the security attributes and takes specified action after detecting the security attributes expiry
O.LOCKOUT	FIA_AFL.1	O.LOCKOUT is fulfilled in the following manner: - FIA_AFL.1.2 restricts the amount of login attempts to an administratively defined number (3-9). When this defined number is met the account is disabled.
O.AUTH_MECH	FIA_UAU.5 FIA_SOS.1	O.AUTH_MECH is fulfilled in the following manner: - FIA_UAU.5 provides a mechanism to accept credentials in the form of MyKad, Biometric, iKey USB Token and Password - FIA_SOS.1 provides enforcement of complex passwords through IAM policies.
O.FILTER	FTA_TSE.1	O.FILTER is fulfilled in the following manner: - FTA_TSE.1 - prevents session establishment based on HTTP request parameters.

Table 14 - Mapping of Security objectives for the TOE to SFRs

5.4 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components to Evaluation Assurance Level 4 (EAL4).

This section contains the assurance requirements for the TOE. The assurance requirements are listed in Table 15, below.

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
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined lifecycle model
	ALC_TAT.1 Well-defined development tools
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.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 15 - TOE Security Assurance Requirements (SARs)

5.5 Assurance Requirements Rationale

This ST claims compliance to the assurance requirements from the CC EAL4 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The TOE is intended to address the common authentication and authorization attacks on the web based applications

5.6 Rationale for not addressing all dependencies

FPT_STM.1 is a dependency of FAU_GEN.1 and FMT_SAE.1 that has not been included. Reliable time stamps are provided by the environment through an interface of the TOE.

6. TOE Summary Specification

This provides the TOE summary specification. The table below illustrates how the MQAssure™/IAM features achieve the TOE Security Functional Requirements

Item	Description
Strong Multifactor User Authentication	
FIA_ATD.1	**User attribute definition** The TOE maintains the following list of security attributes belonging to individual users: a) User name – a unique name for each user b) Type of the authentication scheme assigned to the user – the authentication type for the application and user combination. Based on types defined in FIA_UAU.5. c) User credential for the assigned authentication scheme – the representation of the credential to match to the users input. d) User role – the role of the user as defined in FMT_SMR.1. e) Authentication Failure counter. This counter tracks the number of failed login attempts. f) Status – this attribute tracks the enabled/disabled status of a user [related to their number failed authentication attempts].
FIA_SOS.1	**Verification of secrets** IAM enforces its password complexity policy during the events: a) User/administrator enrolment; and b) Password change. The TOE will enforce the password complexity rules (once configured by the Administrator) which require that passwords: a) include at least one numeric character;

	b) contain at least one special character; c) not contain a repeating predictable sequence; and d) contain minimum number of characters (at least 8)
FIA_UID.2	**User identification before any action** The TOE presents the users and administrators with a login in screen when they first connect to the TOE. Unless a user is successfully identified and authenticated, no actions are permitted for that user.
FIA_UAU.2	**User authentication before any action** The TOE presents the users and administrators with a login in screen when they first connect to the TOE. The user is required to use the authentication configured as part of FIA_ATD.1. Before performing the credential check, the TOE will increment the authentication failure counter. If the counter is greater than the configured limit (FIA_AFL.1), the TOE will not compare the provided credentials and will reject the authentication attempt. Unless a user is successfully identified and authenticated, no actions are permitted for that user.
FIA_UAU.5	**Multiple authentication mechanisms** The TOE accepts credentials in the form of MyKad, Biometric (the verification of biometric fingerprint will happen on reader itself), iKey USB Token and Password. The TOE shall authenticate any user's claimed identity according to the following options a) If the assigned authentication scheme for the user is MyKad/Biometric (see FIA_ATD.1), then the user is prompted to insert his MyKad into the reader and place the thumb over the finger print scanner and the AppShield performs a 1:1 match of the users live fingerprint minutiae against the stored fingerprint minutiae in the MyKad and then verifies the MyKad details with the MQAssure™ /IAM server b) If the assigned authentication scheme for the user is iKey/PIN (see FIA_ATD.1) then the AppShield prompts the user to insert the iKey into the USB port of his PC and enter the PIN to unlock the iKey. If the

	PIN entered is right then the AppShield will be able to unlock the iKey. AppShield will verify whether the iKey serial number inserted is the same with iKey serial number registered for that particular user with MQAssure™ /IAM server. c) If the assigned authentication scheme for the user is user ID and password (see FIA_ATD.1) then the AppShield prompts the user to enter his user ID and password and then sends the password hash to the MQAssure™ /IAM server for verification
FIA_UAU.6	**Re-authenticating** The TOE requires that a user or administrator re-authenticate the user upon Session timeout (see FTA_SSL.3)
FIA_AFL.1	**Authentication failures** The TOE tracks the number of failed authentication attempts made by a user and, prior to authenticating the user, compares them to the number of allowed attempts. If the number of allowed attempts is reached, the user is disabled. The administrator can configure the number of allowed failures to a number between 3 – 9 unsuccessful authentication attempts The default and recommended configuration for unsuccessful authentications is 3. When the defined number of unsuccessful authentication attempts has been met, the TOE shall disable the user account. Administrator can re-enable an account manually through the admin console. Another way is user can enable their own account through answering security questions at the Self Help page.
TOE Administration	
FMT_SMF.1	**Specification of management functions** The TOE allows the administrator to perform the following management functions: a) Identity management- centralized management of identities such as Users, Roles and Resources. The identities are stored in relational database. This includes enabling disabled user accounts. b) Audit reporting- Audit log subsystem provides two

	types of audit function, which are Audit Logon service and Data Transaction Log events. Audit Logon events are login success, login failed, Logout, account locked, session expired. Data Transaction Log events are create, modify, delete, enable, disable and search records. c) Policy management - centrally manage the authentication and authorization policies for the MQAssure™ /AppShield instances deployed. Through the administration console, the authorized administrator can define access policies for various resources. d) Session Services – centralized management of user sessions and continuously monitors the user activities on the session and the session expiry. Each session is maintained for a specific session validity period (configured by Administrator) after which the session expires. The session service ensures the uniqueness and secure generation of the session IDs which is stored in a client cookie for tracking the client sessions.
FMT_SMR.1	**Security roles** The TOE maintains the roles, Users, Administrators and Approvers. These roles are default roles. Users can have one or more access roles based on the organizational access requirement.
FMT_MSA.1	**Management of security attributes** The TOE restricts the ability to change default, create, modify and delete the users security attributes to TOE administrators
FMT_MSA.3	**Static attribute initialization** The TOE ensures that all default values for security attributes (specifically the permissions in the organizational policies) that are used to enforce the SFP are restrictive, e.g. no users have access to an object by default. The TOE allows the TOE administrators to specify

	alternative initial values to override the default values at creation of a new object.
FMT_SAE.1	**Security attribute expiration** The TOE restricts the capability to specify an expiration time for password to TOE Administrators. The TOE disables the user account after the expiration time for the password has passed.
Security Audit	
FAU_GEN.1	**Audit data generation** The TOE generates an audit record when any and all of the following auditable events occurs: a) Start-up and shutdown of the audit functions are not applicable to TOE because TOE audit function is always ON. There is no function to enable/disable an audit function. b) Addition or removal of application resources in the TOE; c) Success or failure of User authentication; d) All the operations (creation, deletion and modification) of the password policies; e) All the operations (creation, deletion and modification) of User profile f) All the operations (creation, deletion, activation and deactivation) of User Role; The TOE record within each audit record the Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and severity.
FAU_GEN.2	**User identity association** The TOE associates each auditable event with the identity of the user that caused the event for audit events resulting from actions of identified users, by storing their user name in the audit log.
FAU_SAR.1	**Audit review**

	The TOE provides TOE Administrators with the capability to read audit time stamp, audit details, subject of the audit event and audit severity from the audit records, through the admin console. The TOE provides audit records in a simple list that allows administrators to read them.
FAU_SAR.2	**Restricted audit review** The TOE only permits users read access to the audit records, if they have the appropriate permission.
FAU_ARP.1	**Audit automatic response** The TOE shall email an alert message to administrator upon detection of a potential security violation. The security violation are defined as per FAU_SAA.1.
FAU_SAA.1	**Potential violation analysis** The TOE applies a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs. The TOE will detect an accumulation or combination of repeated logon failure, repeated unsuccessful access requests (accessing unauthorized URL) known to indicate a potential security violation.
FTA_TAH.1	Upon successful session establishment, the TOE displays the date, time, method and location of the last successful session establishment to the user. Upon successful session establishment, the TOE displays the date, time, method and location of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. The TOE does not erase the access history information from the user interface until the user acknowledges the alert.

Table 16 - Security features of MQAssure™/IAM

The table below illustrates how the MQAssure™/AppShield features achieve the TOE Security Functional Requirements

SFR	How achieved
Access Control and HTTP request validation	
FDP_ACC.1	**Subset access control** The TOE shall enforce the access control policies on Subjects (User, Role), Objects(Resource, Audit Logs) and Operations(Read, Write, Delete) covered by the SFP.
FDP_ACF.1	**Security attribute based access control** The TOE shall enforce the access control policies to objects based on the following: <u>Subject:</u> - Role – role name, business unit, permissions - User – User name, password, organization unit, role, location <u>Objects:</u> - Resource – Resource Name, Resource ID, Resource IP, Resource Port - Audit Log – Audit Log ID, Audit Time The TOEshall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: a) Evaluate the attributes of subjects and objects against the policies on the IAM server - Operation is allowed if the policy explicitly grants permission - Operation is denied of the policy explicitly denies the permission - If there is no matching policy then the default action is to deny permission The TOE has no additional rules in governing explicitly authorise access or deny access of subjects to objects.
FTA_SSL.3	**TSF-initiated termination**

	The TOE terminates an interactive session after a specified time of user inactivity, based on administrator's configurations in admin console.
FTA_MCS.1	**Limits on multiple concurrent sessions** The TOE shall restrict the maximum number of concurrent sessions that belong to the same user. By default, a limit of 1 session per user is enforced.
FTA_TSE.1	**TOE session establishment** AppShield will prevent session establishment based on the following: a) IP address; and b) HTTP request parameters.

Table 17 - Security features of MQAssure™/AppShield

Appendix - A

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
MyKad/Biometric	Authentication scheme that is using combination of smart card and user fingerprint. Also denoted as MyKad-Biometric.
iKey/PIN	Authentication scheme that is using combination of usb token and its pin number. Also denoted as iKey-PIN.
User name/password	Authentication scheme that is using combination of User name and password. Also denoted as User name-password.