Ref: 2014-04-14-ST-SCANS_S3-v2.7
Author: Siswaco Sdn Bhd (978808-T)

SCAN S3 Security Target

DOCUMENT VERSION	V2.7
DOCUMENT DATE	14 APR 2014

SCAN Associates Berhad
Level 7, MenaraAtlan,
161-B, JalanAmpang,
50450 Kuala Lumpur
Email: corpcomm@scan-associates.net
Tel: (603) 2166 0020
Fax: (603) 2166 1020
Website: http://www.scan-associates.net

DOCUMENT REVISION HISTORY

Version No.	Author Initial	Published Date	Description of changes
v1.0	SCAN/SISWACO	16 April 2013	First Issue
v1.1	SCAN/SISWACO	19 April 2013	Update Diagram Logical Scope
v1.2	SCAN/SISWACO	15 July 2013	Update Diagram Logical Scope
v2.0	SCAN/SISWACO	23 July 2013	Update the scope of TOE and Logical Scope Diagram – Major Changes
v2.1	SCAN/SISWACO	29 July 2013	Minor update on the info.
v2.2	SCAN/SISWACO	31 July 2013	Minor update on the info.
v2.3	SCAN/SISWACO	02 August 2013	Minor update on the info.
v2.4	SCAN/SISWACO	01October 2013	Minor update on the info.
v2.4	SCAN/SISWACO	15 Nov 2013	Minor update on the info. No version changes on the document.
v2.5	SCAN/SISWACO	25 Feb 2014	Update based on EOR03.
v2.6	SCAN/SISWACO	02 April 2014	Update based on EOR04.
v2.6.1	SCAN/SISWACO	04 Apr 2014	Update version of S3 Agent to v2.0.1.6.2
v2.7	SCAN/SISWACO	14 Apr 2014	Final version

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	SCAN S3 Security Target
Security TargetVersion:	v2.7
TOE Software Identification:	SCAN S3 Security Manager Console Release 14556 (v2.0)
	*İntegratedwithSCAN*S3 Agent (v2.0.1.6.2)
Evaluation Assurance Level:	EAL2

Table 1: ST Reference

1.2 TOE Reference

TOE Name & Version	**TOE NAME:**	**TOE VERSION:**
	SCAN S3 Security Manager Console Release 14556 (SCAN S3 SMC)	v2.0
	SCAN S3 Agent	v2.0.1.6.2
TOE Initial:	SCAN S3 SMC-AGENT or SCAN S3	

Table 2: TOE Reference

1.3 Terminology and Acronyms

TOE	Target of Evaluation
TSF	TOE Security Functionality
CLI	Command Line Interface
LAN	Local Area Network
TLS	Transport Layer Security
SSH	Secure Shell
Webconfig	Web interface for TOE administration purpose
IP	Internet Protocol

NTP	Network Time Protocol
OSP	Organizational Security Policy
OTP	One Time Password

1.4 Reference

CCPart1 Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

CCPart2 Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

CCPart3 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

CEM Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

1.5 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.5.1 Usage and Major Security Features of the TOE

SCAN S3 Security Manager Console (SCAN S3 SMC for short) integrated with SCAN S3 Agent, is the product developed by SCAN Associates Bhd to assist in designing, implementing and maintaining a coherent suite of processes and systems for effectively managing information accessibility.

SCAN S3 SMC-AGENTis a platform that consolidates various security services into a single enterprise-wide architecture. SCAN S3 SMC-AGENThelps to mitigate the security risks when implementing an Enterprise Application and e-Services.

In traditional implementations, clients or customers will need to have different accesses to different products or systems and the management of these separate application accesses can be an administrative burden. This also can lead to unnecessary exposure to security leakages if accesses to different systems that are linked or integrated are not implemented according to a consistent policy.

With the multiple options or permutations available in the above implementation, the SCAN S3 SMC-AGENTenables the organization to manage the overall security through a single framework that enables the defining and assignment or implementation of the following security functions in one system:

a) Security Audit;
b) Authentication and Identification;
c) Cryptography;
d) Security Management;
e) User Data Protection; and
f) Protection of the TSF.

Additionally, with the new enhancement made into the SCAN S3 SMC-AGENT, users are better protected and secured from any types of networking (internal and external) threats within the systems operational environment based on PKI implementation through software desktop, , soft-certificates, roaming certificates and smart cards, integrated directly to the SCAN S3 SMC-AGENT server system via networking capabilities.

1.5.2 TOE Type

SCAN S3 SMC-AGENT is a Web-Based Application Access Control Management, which enable users to access their internal network resources securely through PKI implementation via soft-certificates, roaming certificates and smart cards. SCAN S3 SMC-AGENT is the combination of SCAN S3 SMC (Security Management Console), in which, the SCAN S3 SMC is define as the administration console for the operations SCAN S3 SMC-AGENT in the aspects of managing users and the access controls, thus, as for the SCAN S3 AGENT is the front-end interface for all users registered in the SCAN S3 SMC system, uses the interface as a secure platform in communicating with the protected resources govern by the security protection of SCAN S3 SMC-AGENT.With the new integration of software desktop that enable users to access the internal network resources, by inputting soft-certificate, roaming certificates orsmart cards through that application.

1.5.3 Non-TOE Software, Hardware and Firmware

Below is the list of non-TOE requirements:

Requirements	Descriptions	Version & Specifications
Server System and Software Requirements		
Hardware	Server	Intel (R) Pentium (R) M Processor 1.60 GHz, 220 MHz, 2.00 GB of RAM
Software	Operating System	Ubuntu Server 12.04 or Windows 2003 Server SP2
	Application	a) Tomcat 7.0 - Tomcat Application Server; or b) Enterprise Java Beans (EJB) Application server that hosts all the software and Application for the system component
	Database	MySQL 5.5Database
Client System and Software Requirement		
Hardware	Desktop	Intel (R) Pentium (R) M Processor 1.60 GHz, 220 MHz, 2.00 GB of RAM
	Mouse/Pointing Device	Any pointing device with at least 2 buttons
Software	Operating System	Windows XP Service Pack 2, Windows Vista, Windows 7
	Web Browsers	Mozilla Firefox [v7.1] Internet Explorer [v9.0]

Requirements	Descriptions	Version & Specifications
	Monitor Resolution	SVGA – Compatible display (256 or more colours recommended) with resolution of at least 1024 x 768 pixels
	Archive Utility	WinZip or equivalent
	Application Documentation	Adobe Acrobat Reader (4.0 or higher) to read online PDF files.
	Java Requirements	JRE 1.7 and above
Tokens	Smart Card	Stored with digital certificate of user (Read Only)
	Soft Certificate	Digital certificate provided by trusted entity or organization to user.
	Roaming Certificate	Digital certificate provided by trusted entity or organization to user via request from a portal that shall release the certificate temporary for certain usage at certain period of time.

Table 3: None-TOE Software, Hardware and Firmware

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope of the TOE

The SCAN S3 or SCAN Shared Security Services comprises two (2)components or services:

a) SCAN S3 Security Manager Console (SCAN S3 SMC); and
b) SCAN S3 Agent.

All of these components is part of the scope of TOE, in which, functioning based on integration all together in its operational environment that shall be described in the TOE Guidance documentations. Note that, all hardware and software stated in Section 1.5.3 is not part of the TOE, and known as supporting components to the TOE operational environment.

Moreover, the details elaboration of SCAN S3 components as stated below:

a) SCAN S3 Security Manager Console (SCAN S3 SMC).
The SCAN S3 SMC, which is the first element of the TOE, is the security administration console to set up the user authorization parameters, defining the user's authentication mode as well as the workstation and risk policy.The following describes the features of SCAN S3 SMC:
    - Centralized administration of logon ID's.
    - Centralized policy configuration.
    - Centralized collection of logging of events.

   TOE Administrator/s isapplicable to work with different types of roles, responsibilities, access privileges and access rights based on their job descriptions. Such example, there will be a TOE Administrator with less accessibilityinto theTOE plus with limited access privilegesinto the TOE modules or functions.

b) SCAN S3 Agent:
It is a Software desktop component that provides PKI related functions (importing certificate, removing certificate, listing all loaded certificates, signing user data, verification of signing data and user credential, authentication components, and checking for roaming certificate usage (for user that assigned with the roaming certificate usage)) at client side.The following describes the features of SCAN S3 Agent:
    - Installed at client side, which is, client desktop workstation.
    - Other than integrated with SCAN S3 SMC, third party application could invoke the PKI function by using HTTP GET protocol via JavaScript (JQuery).

Support several devices platform usage of certificates (soft certificate, roaming certificate, and smart card). User is not allowsto use more thantwo types of the certificate or tokens. Such example, user can be assigned by TOE Administrator/.In general terms of explaining the SCAN S3 or known as SCAN Shared Security Services, are design based on the principles as follows:

a) It is positioned as a 'platform' and not designed to be stand alone;

b) Completely Web Services implementation;
c) Compliance to Malaysian Government's classified information handling handbook – "BlackBook";
d) Risk based authentication; Supports multiple authentication mechanisms; and
e) PKI key is use as an authentication component for accessing protected resources through the roaming operations. This is known as roaming PKI certificate processes.

Furthermore, with the new enhancement made on to the existing SCAN S3 SMC, which is to include SCAN S3 Agent, allowing user to access the TOE through alternative method rather using the conventional method through web browser authentication and identification process. The SCAN S3 Agent as software desktop allows users to use PKI infrastructure that consist of usage in soft-certificates, smart cards and roaming certificates.

The following figure illustrates the operations of TOE. Figure 1 illustrates one of example of TOE deployment in the client side.

General descriptions of Figure 1:

- SCAN S3 SMC shall be maintained, configured and monitored by Admin. It is recommended to have minimum two (2) Admin personnels, which is, one from the developer and one from the Headquarter (HQ).
- SCAN S3 AGENT users did not see or able to access the SCAN S3 SMC during the PKI implementation at the protected websites bound back to the SCAN S3 SMC-AGENT implementation and operational environment.
- SCAN S3 SMC is located and deployed at theHQ site, in which, all operations environment for SCAN S3 SMC are govern by the organizational security policiesimplementationof the HQ.
- SCAN S3 AGENT is deployed and installed at all HQ clients'workstations that are registered by AP. AP shall registered users that will be using PKI solution provided by SCAN S3 SMC-AGENT, and assist with the SCAN S3 AGENT software desktop.
- Licensed Certificate Authority (CA) is not part of the scope of TOE, and only operates by supplying SCAN S3 SMC with new generation of digital certificates, revocation status of digital certificates and related processes on the operational environment of PKI issuance.
- All SCAN S3 AGENT users will be authenticated and identified by SCAN S3 SMC by enforcing usage of digital certificates through soft certificate, roaming certificate and/or smart card token. The processes authentication and identification (username/user ID+ password/PIN + PKI) are internal process performed by SCAN S3 SMC.
- SCAN S3 SMC will communicate with Licensed CA servers on the PKI validation and send back notification/status back to the SCAN S3 SMC server, proceeding with the user's authentication and identification processes. If all requirements successful validated, SCAN S3 SMC will send the status to SCAN S3 AGENT, allowing users to proceed accessing the protected website enforced by SCAN S3. Admin of SCAN S3 SMC is requiresto register the list of website that will be enforced by SCAN S3.

- Note that, Authentication Service is located under Authentication Server; Roaming Service is a module of SCAN S3 SMC that handles roaming certificate processing; and Certificate Repository Server is a mirror server at SCAN S3 site to store temporary certificates, request certificates and acknowledge certificates from Licensed CA Servers.

Disclaimer: SCAN S3 SMC-AGENT are applicable to be deploy in different operational environment that may have more components or less components as stated in Figure 1, shall be noted as not part of the scope of TOE. If such deployment is been performed, developer shall not be blame or taking any responsibility if the deployment produced vulnerabilities and flaw. Any deployment of the SCAN S3 SMC-AGENT shall be advice by developer in making sure that the SCAN S3 SMC-AGENT are properly deploy in its secure operational environment.

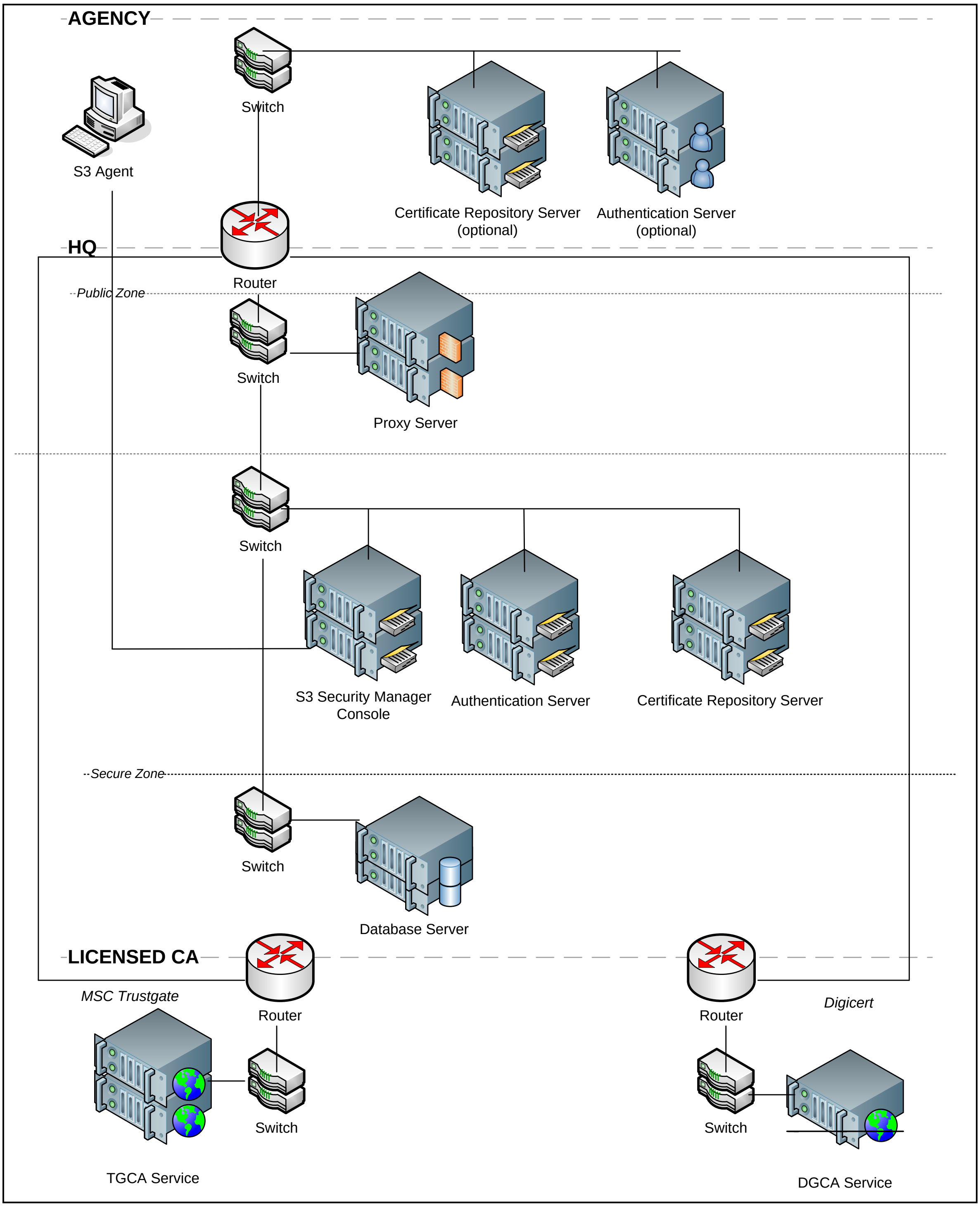

Figure 1: TOE Physical Scope

1.6.2 Logical Scope of the TOE

The logical scope of TOE is described based on several security functional requirements as below.

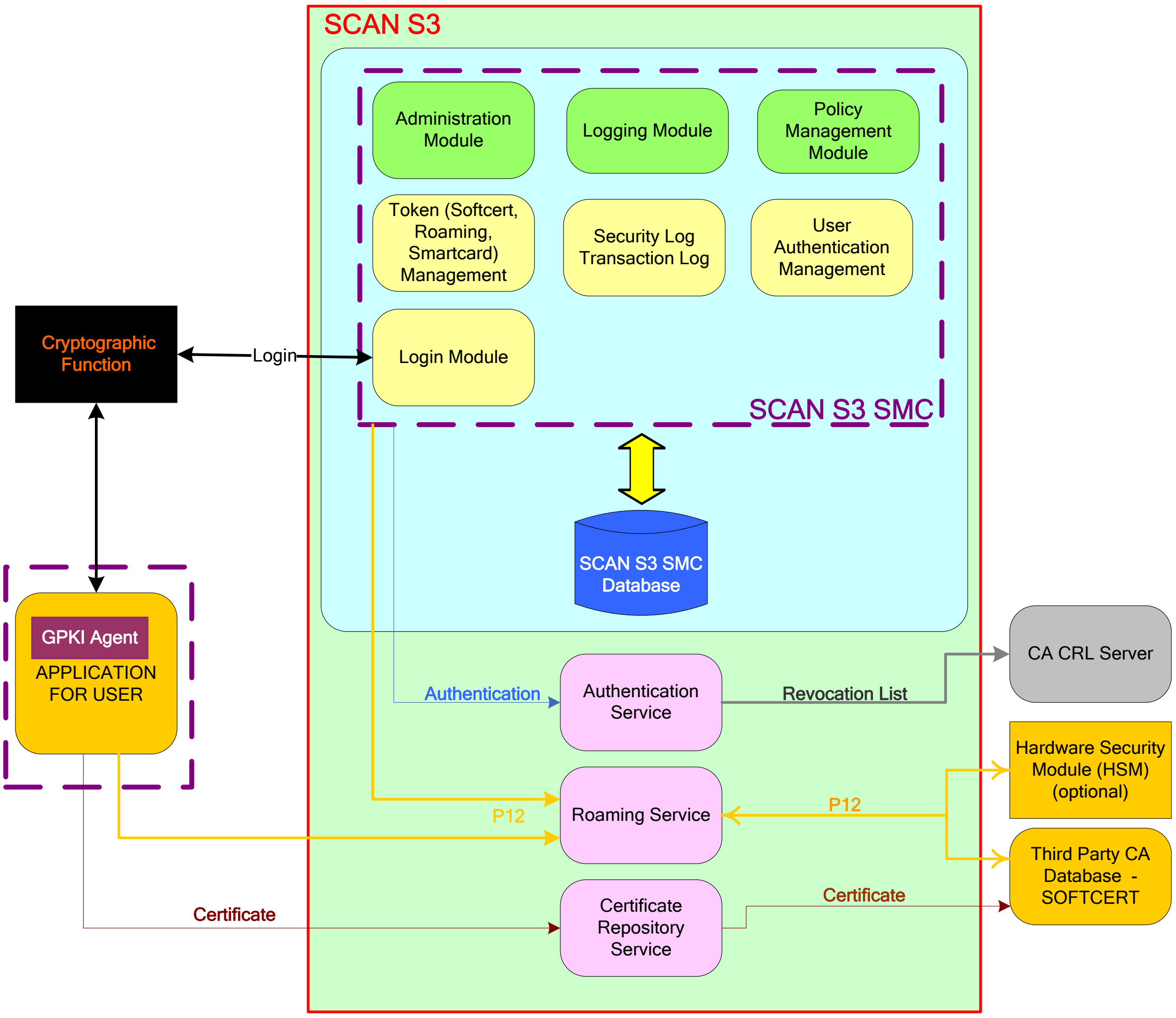

Figure 2: Scope of TOE

Based on the notes given in the Figure 2, all within the **PURPLE DASHED**(SCAN S3 SMC & SCAN S3 Agent) are declared as part of TOE scope. Kindly ignore the colouring within the boxes, which is, only illustrate the boundary of operations that relates to modules functions within SCAN S3 SMC.

Details explanation of the SCAN S3 AGENT is described in the Physical Scope, Logical Scope (Section Authentication and Identification; Section Cryptography) and TOE Summary Specification (Section Authentication and Identification; Section Cryptography).

As for SCAN S3 SMC details, it is provided inside the Physical Scope descriptions, as well as, in the Logical Scope and TOE Summary Specifications.

1.6.2.1 Security Audit

The TOE will generate audit records for selected security events in several log files and categories. Each audited events will be recorded along with date and time of event, user accounts that performed the event, event name and other event details. Audit records can be viewed by TOE Administrator/s and cannot be edited. TOE Administrator/scould select and filter the logs for easy viewing. TOE will create a new log file and may overwrite the old audit log records to store the audit records if the size limit is reached for a log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE hardware server. Note that, TOE Administrator/s shall be advice to backup all logs that is crucialtothe TOE operational environment in accordance to organizational security policies in protecting the logs from any damages or tampering or loss.

The security audit function ensures that all TOE Administrator/s activities pertaining to creation/update/delete of TOE Administrator/s, as well as the assigning TOE Administrator/sroles and privilege accessibilitiesshall be log by audit functions. Details of audit logs and management of audit components are being explained in the Guidance documentations. Types of logs and descriptions of logs are described in details at TOE Summary Specification (TSS).

1.6.2.2 Authentication and Identification

All TOE Administrator/smust have a valid username/user ID, password/PIN and PKI tokens (soft certificate, roaming certificate and/or smart card). Each user shall be assigned with minimum of two (2) types of PKI among the stated PKI types.

TOE Administrator/smust login to SCAN S3 to identify themselves to the application together with the prompted (one of up to three) authentication means in order for them to gain access to the protected websites, using SCAN S3 AGENT software desktop. With the new enhancement made throughS3 Agent software desktop, all Administrators and Users shall require to use their own assigned PKI tokens (soft certificate, roaming certificate and smart card) in the authentication and identification processes.

In aspects of access control and session established upon authentication and identification, each user are given 20 minutes idle mode. This feature is configurable based on the policies defined by the organization security policies. If a login session has remained idle for 20 minutes, the user will have to re-login to access the application again.

By default, TOE Administrator/s (Admin) can use a built-in administrative account known as “admin” used for authenticating throughTOEweb application portal. TOE Administrator/s will be granted role based on built-in Groups, access to services and pages within web application portal. TOE Administrator/s are able to modify the existing configurable settings as per required. However, there are several built-in features could not be modified by TOE Administrator/s.As for SCAN S3 AGENT user/s will not be seeing or accessing or have access to SCAN S3 SMC directly and not allowed doing so.

1.6.2.3 Cryptography

TOEhas a built-in feature of cryptography that bound to the operations of SCAN S3 AGENT at Users and Administrators workstation. Each of them is required to install the SCAN S3 AGENT before initiating communication with the SCAN S3 SMC components via web browsers.

The SCAN S3 AGENT has the capabilities of performing cryptographic functions such as Import certificate, removing certificate, capturing certificate from PKI token, listing all certificates, signing, verification, authentication and checking for roaming certificate at client side in their workstation or desktop. Where else, in the operational environment of roaming certificate, SCAN S3 AGENT shall become handler of the process of roaming certificate during authentication and identification processes, as well as, other cryptographic operations within the TOE boundary operations. SCAN S3 AGENT for SCAN S3 SMC-AGENT supports soft certificate, roaming certificate and smart card.

1.6.2.4 Security Management

TOE Administrator/s has access to all TOE features, that applicable to be managed through web application portal hosted byTOE.TOE is able to provide accessibility of multiple types of account that has access privilege, similar or limited,to “Admin” account. In which, Admin account has the full access rights, role and privileges to the TOE.TOE Administrator/s could enable, disable and modify the behaviour of services controlled by TOE, user attribute values, network settings, time-of-day web access, NTP Time Server, backup and restore configurations setting and related functions of TOE.

Operations of Security Management features are performed by User Management module, Token Management module, Administrationmodule, Logging module, Policy Management module, User Authentication Management and Login Module.

1.6.2.5 User Data Protection

User/s data and credentials including TOE Administrator/s information is protected by ensuring that specific TOE Administrator/s that is assigned with roles and privilegescan only access a specific web pages/portals and hence the data associated with the web pages/portal. The accessibility of the pages/portals is protected based upon theInformation flow control policy. The information flow control policy allows the TOEAdministrator/sto create username/user of the normal users that is assigned to access the TOE protected web applications.

TOE has the capabilities of enforcing protection upon resources that the TOE protected,by implementing access control protection on authentication and identification webpage (login page) by using information flow controls through access control policy. The TOE will check for legitimate access control credentials such as username/user ID, password/PIN and PKI’s components (soft certificate, roaming certificate or smart card) before allowing such credentials to access the web applications portal protected by the TOE. TOE Administrator/s could manage and configure access control policy by PKI types selections and privilege access control, are defined to specific user account accessibility. By default, users without any access control credentials are not allowed to access the protected resources.

1.6.2.6 Protection of the TSF

The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. As for the TOE, the timestamp are taken from the underlying operating system.

2 Conformance Claims

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

CCv3.1 conformant
The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 4.

Part 2 conformant
The ST is Common Criteria Part 2 extended

Part 3 conformant
The ST is Common Criteria Part 3 conformant

Package conformant
The ST is package conformant to the package Evaluation Assurance Level EAL2.

Protection Profile conformance
None

3 Security Problem Definition

3.1 Assumption

The assumptions are made to ensure the security of the TOE and its deployed environment.

A.PHY	The TOE and its environment are physically secure and managed by authorized TOE Administrator.
A.FLOW	Data and information could not flow through between internal and external networks and vice versa, unless it passes through the TOE.
A.ADMIN	Authorized TOE Administrator/s is non-hostile and follows guidance documentation accordingly; however, TOE Administrator/s is not free from human error and mistakes.
A.TIMEBACK	The TOE environment will provide reliable time stamps and backup storage enough for TOE supporting operational environments.
A.MGMT	The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that secure and trusted connections can be established to the management network (i.e. through a trusted VPN or trusted Virtual LAN).
A.CONN	Authorized TOE Administrator/s will access the TOE using a secure connection.
A.USER	Unauthorized user who is not authorized TOE Administrator/s cannot access the TOE remotely from the internal or external networks or trusted networks.

Table 4: TOE Assumptions

3.2 Threats

Assets that are protected by the TOE are sensitive data, stored in the TOE and internal network including critical TOE configuration data (configuration files, user’s credential and others), audit records, administrator credentials, TOE data and TOE security functions.

Threat agents are entities that can adversely act on the assets. The threat agents identified are an unauthorized person and an authorized administrator (a person that has been successfully authenticated and authorized as an administrator).

Threats may be addressed either by the TOE or by its intended environment.

T.ACCESSLOG	An unauthorized person successfully accesses the TOE data or security functions without being detected.
T.AUDIT	An unauthorized person or authorized TOE Administrator/s may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.
T.EXPLOIT	An unauthorized person may send impermissible information through the TOE that result in the exploitation of protected resources.
T.REMOTE	An unauthorized person or unauthorized external IT entities may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized TOE Administrator/sdesktop and the TOE.
T.CONFIG	An unauthorized person may read, modify, or destroy TOE configuration data.
T.NOAUTH	An unauthorized person may attempt to bypass the TOE access controls, in accordance to modify current existing security configurations, provided by the TOE.
T.SPOOF	An unauthorized person may carry out network spoofing and/or sniffing activities, in which, information flows through the TOE into a connected network by using a spoofed source address.

Table 5: TOE Threats

3.3 Organizational Security Policy

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

P.ROLE	Only authorized individuals are assigned by the organization have access to the TOE.
P.PASSWORD	Authorized TOE Administrator/s shall use/create password with combination of special character, number and alphabet with minimum lengths of 12 that defines a good and hard to guess password, whilst, in mitigating password-guessing activities.

Table 6: TOE OSP

4 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its environment will meet these objectives.

4.1 Security Objectives of TOE

The security objectives for the TOE as following:

O.ACCESSLOG	TOE shall record a readable log of security events.
O.AUDIT	TOE shall prevent an unauthorized person or authorized TOE Administrator/s to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.EXPLOIT	TOE shall mediate the information flow between users and protected resources intended based on user requested.
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data.OnlyauthorizedTOEAdministrator/s shall have access to TOE management interface.
O.NOAUTH	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.

Table 7: Security Objective for the TOE

4.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

OE.PHY	The TOE and its environment shall be physically secure.
OE.FLOW	The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
OE.ADMIN	Authorized TOE Administrator/s shall be non-hostile and follow guidance; however, TOE Administrators is not free from human error or mistakes.
OE.TIMEBACK	The TOE environment shall provide reliable time stamps and backup storage enough for TOE supporting operational environments

OE.MGMT	The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, enforced with HTTPS).
OE.CONN	Authorized TOE Administrator/s shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.
OE.USER	Unauthorized user who is not authorized TOE Administrator/s cannot access the TOE remotely from the internal or external networks.
OE.SOFTCERT	Authorized TOE Administrator/s shall be able to keep and secure the soft certificates in the secure location (logically or physicaly) and performed regular backup of those soft certificates.

Table 8: Security Objective for the Operational Environment

5 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE. These requirements are presented following the conventions identified in Section 6.1 Conventions.

5.1 Extended Security Functional Requirement (SFR)

Extended Component	Extended Component Name	Rationale
Class FAU : Security Audit		
FAU_GEN.3	Simplified Audit Data Generation	FAU class contains families of functional requirements that are related to monitor security-relevant events, and act as a deterrent against security violations. This component is a member of FAU_GEN, an existing CC Part 2 family. This extended requirement for the FAU class has been included in this ST because TSF audit function does not log start and stop of auditing function; henceFAU_GEN.1.1 (a)is not applicable. This component is also created to simplify the requirement of FAU_GEN.1.
Class FPT: Protection of the TSF		
FPT_STM.2	Reliable time stamps by operational environment	FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. This component is a member of FPT_STM, an existing CC Part 2 family. This extended requirement for the FPT class has been included in this ST because the operational environment is providing reliable time stamps for TSF functions that are not covered in FPT_STM.1.

Table 9: Extended Component Description

5.1.1 Class FAU: Security Audit

FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other component

Dependencies FPT_STM.2 Reliable time stamps by operational environment

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:

[**assignment: defined auditable events**].

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event

b) [**assignment: other information about the event**].

5.1.2 Class FPT: Protection of the TSF

FPT_STM.2 Reliable time stamps by operational environment

Hierarchical No other component

Dependencies No other dependencies

FPT_STM.2.1 The operational environment shall be able to provide reliable time stamps for the TSF functions.

5.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

6 TOE Security Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 Conventions

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

Assignment The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows[**assignment**].

Selection The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

Refinement The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

Iteration The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing an acronym at the end of the component identifier as follows: FCS_COP.1 (SWP).

6.2 Security Functional Requirements (SFR)

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Component	Component Name
Class FAU : Security Audit	
FAU_GEN.3	Simplified Audit Data Generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restrictedauditreview
FAU_STG.1	Protectedaudittrailstorage
FAU_STG.4	Prevention of audit data loss
Class FCS: Cryptographic Support	
FCS_COP.1	Cryptographic operation
Class FDP : User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
Class FIA :IdentificationandAuthentication	
FIA_ATD.1	User attributesdefinition
FIA_UAU.2	User authenticationbeforeanyaction
FIA_UID.2	User identificationbeforeanyaction
FIA_USB.1	User-subjectbinding

Class FMT : Security Management	
FMT_MOF.1	Management of securityfunctionsbehaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of securityattributes
FMT_MSA.3	Staticattributeinitialisation
Class FTA: TOE Access	
FTA_SSL.1	TSF initiatedsessionlocking
Class FPT : Protection of the TSF	
FPT_STM.2	Reliable time stampsbyoperationalenvironment

Table 10: Security Functional Requirements List

6.2.1 Class FAU: Security Audit

FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other component

Dependencies FPT_STM.2 Reliable time stamps by operational environment

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:[

a) **All auditable events for the basic level of audit;**

b) **Process flow of authentication will be logged; and**

c) **Management of the TOE. Example, change of role, add user, edit user.**

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:[

a) **Date and time of the event;**

b) **Type of event;**

c) **Subject (users) identity;**

Application notes None

FAU_GEN.2 User identity association

Hierarchical No other component

Dependencies FAU_GEN.3 Simplified audit data generation

FIA_UID.1 Timing of identification

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.

Application notes None

FAU_SAR.1 Audit review

Hierarchical	No other component
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [**TOE Administrator/s**] with the capability to read [**all audit logs trail data**] 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.
Application notes	This dependencies are met by FAU_GEN.3

FAU_SAR.2Restricted audit review

Hierarchical	No other component
Dependencies	FAU_SAR.1 Audit review
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.
Application notes	None

FAU_STG.1 Protected audit trail storage

Hierarchical	No other component
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.
Application notes	This dependencies are met by FAU_GEN.3

FAU_STG.4Prevention of audit data loss

Hierarchical	FAU_STG.3 Action in case of possible audit data loss
Dependencies	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [**append the oldest stored audit records**] and [**none**] if the audit trail is full.
Application notes	None

6.2.2 Class FCS: Cryptographic Support

FCS_COP.1Cryptographic operation

Hierarchical	No other component
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [**authentication, verification and signing]**in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048]** that meet the following: [**X.509**].
Application notes	Referring to: http://en.wikipedia.org/wiki/Digital_signature http://en.wikipedia.org/wiki/Public_key_certificate Key generation and destruction are performed by the Licenced CA. Therefore, the dependencies of FCS_CKM.1 is not applicable because of the Key generation and Management are performed by the Licensed CA.Communication is link through a secure trusted network between SCAN S3 SMC and CA servers.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical	No other component
Dependencies	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**access control policy**] on [**Table 11**].

Application notes

Objects	Operations	Subjects
User Authentication Management and Login Module	Enable to create, delete and update accounts created in TOE, related to user account credentials and roles/privileges.	TOE Administrator/s
Logging Module	Enable to viewing logs of all activities performed by user accounts and TOE. The logs will have details on all activities.	TOE Administrator/s
Token Management module	Assigning users to their PKI's components. Each user shall have only two PKI components.	TOE Administrator/s
Administrationmodule	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among the TOE operations.	TOE Administrator/s
Policy Management module	Create, delete, enable and disable policy access control and management of other types of data accessibility related to TOE operations.Also, this module able to manage timeout	TOE Administrator/s

	session on the TOE.	

Table 11: Subject, Object and Operations for FDP_ACC.1

FDP_ACF.1 Security attribute based access control

Hierarchical	No other component
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [**access control policy**] to objects based on the following: [**TOE Administrator/s, users and groups that are associated with subject as stated in Table 11**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[a) **IfTOEAdministrators/Users is successfully authenticated according to access privilege assigned, then access are granted based on privilege allocated for that users; and** b) **If user attempt are not successful, therefore, access permission is denied**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Application notes	None.

FDP_IFC.1 Subset Information Flow Control

Hierarchical No other component

Dependencies FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[information flow control policy**] on[**Table 12**].

Application notes

Objects	Operations	Subjects	Information
User Authentication Management and Login Module	Enable to create, delete and update accounts created in TOE, related to user account credentials and roles/privileges.	TOE Administrator/s	User data and credentials
Logging Module	Enable to viewing logs of all activities performed by user accounts and TOE. The logs will have details on all activities.	TOE Administrator/s	Audit logs
Token Management module	Assigning users to their PKI's components. Each user shall have only two PKI components.	TOE Administrator/s	Information on PKI tokens (smart card, soft certificate and roaming certificate)
Administrationmodule	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among	TOE Administrator/s	Information related to TOE operations that links to all

	the TOE operations.		TOE modules
Policy Management module	Create, delete, enable and disable policy access control and management of other types of data accessibility related to TOE operations. Alse, this module able to manage timeout session on the TOE.	TOE Administrator/s	Information of policy enforcement applicable and enforce within TOE operations

Table 12: Subject, Object, Operations and Information for FDP_IFC.1

FDP_IFF.1 Simple Security Attributes

Hierarchical No other component

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [**information flow control policy**]based on the following types of subject and information security attributes: [**refer to Table 12**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlledsubjectand controlled information via a controlled operation if the followingrules hold: [**refer to Table 12**].

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**None**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**None**].

Application notes None

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical No other component

Dependencies No dependencies

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

a) **Username/User ID;**

b) **Password/PIN;**

c) **PKI Token (Smart Card/Soft Cert/Roaming Cert)**].

Application notes None

FIA_UAU.2 User authentication before any action

Hierarchical 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 notes None

FIA_UID.2 User identification before any action

Hierarchical 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.

Application notes None

FIA_USB.1 User-subject binding

Hierarchical No other components.

Dependencies FIA_ATD.1 User attribute definition

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

a) Username/User ID;

b) Password/PIN;

c) PKI Token (Smart Card/Soft Cert/Roaming Cert)].

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

a) Authentication and Identification shall be enforced upon Staff (User) and TOE Administrator/s when accessing protected resources and TOE; and

b) TOE Administrator/sand User/s shall use SCAN S3 AGENT software desktop accordingly upon authentication and identification processes as per requested by TOE].

FIA_USB1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:[**changes of configuration on the TOE only performed by TOE Administrator/s**].
Application notes	None

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical No other component

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable and modify***] the functions [**TOE Configurations**] to [**TOE Administrator/s**].

Application Note TOE configurations is all functions that are applicable for TOE Administrators for modification, disable and enable relevant functions of TOE, whereby, TOE functions are list of configurations menu are editable or selectable values are made available for TOE Administrator/s to perform relevant actions based on organization requirements on the operational environment of the TOE.

FMT_MTD.1 Management of TSF data

Hierarchical No other component

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [***query,[view]***] the [**TOE logs**] to [**TOE Administrator/s**].

Application Note None

FMT_SMF.1 Specification of Management Functions

Hierarchical No other component

Dependencies No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**refer to Table 12**].

Application Note None

FMT_SMR.1 Security roles

Hierarchical No other component

Dependencies No dependencies.

FMT_SMR.1.1 The TSF shall maintain the roles Administrator[**TOEAdministrator/s**].

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

Application Note By default, TOE Administrator/s account that is newly created will have limited access to the TOE. It is up to the default administrator account to give access to specific pages in the web-based administration portal and access to core functions of TOE.

FMT_MSA.1 Management of security attributes

Hierarchical No other component

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 [**assignment: access control policy**] to restrict the ability to [***selection: change_default, query, modify, delete, [view, add]***] the security attributes [**Username/User ID, password/PIN, PKI attributes, TOE Configuration File, TOE Administrator/s, User/s, logs**] to [**TOEAdministrator/s**].

Application Note Details on the security attributes, kindly refer to Table 12.

FMT_MSA.3 Static attribute initialisation

Hierarchical No other component

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 [***permissive***] default values for security attributes that are used to enforce the SFP.

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

Application Note None.

6.2.6 Class FTA: TOE access

FTA_SSL.1 Basic limitation on multiple concurrent sessions

Hierarchical No other component

Dependencies FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after [**TOE Administrator/s configurable20 minutes of user inactivity**] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [**re-authentication**].

Application Note None.

6.2.7 Class FPT: Protection of the TSF

FPT_STM.2 Reliable time stamps by operational environment

Hierarchical No other component

Dependencies No other dependencies

FPT_STM.2.1 The operational environment shall be able to provide reliable time stamps for the TSF functions.

Application Note Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.3.

6.3 TOE Security Assurance Requirements (SAR)

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

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 a 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.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage

Assurance Class	Assurance components
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 13:SAR

7 TOE Summary Specifications

7.1 Security Audit

Audit trail data types as stated below are generated from the logging module within the operations of TOE. These would be sufficient for the TOE Administrator/s to review and generate reports.

SCAN S3 SMC provides 2 types of logging which captures the time, date and associated initiator of the record, i.e. user or system:

Type of Log	Details
Token Activity Log	Transaction logs records all the transaction performed by SCAN S3 services that related to token activities, which are: • Token registration • Document verification • Token approval. • Activation Code generation • View list of users for certain application • Delete token for specific users
Security Log	Application would generate logs for security related events which are: ▪ All Login failures; ▪ Use of administrator and user accounts i.e.Administrator, Log Administrator; ▪ Changes to administrator permissions or privileges; ▪ Creation/deletion/disabling/enabling of all (administration) accounts.

Table 14: Types of TOE Logs

SCAN S3 SMC log entries contain the following details:

- Id – Username/User ID/ Workstation ID;
- Date – date and time of activities;
- IP Address – IP Address of the workstation/ server;
- Detail log of information

The logging can be enabled or disabled by the TOE Administrator/sby manual editing of log4j.properties file via secure access to the TOE workstation. The TOE Administrator/s will also be able to do housekeeping of the logs by performing backup or archiving audit records to external location storagebased on a specified time window, through secure access to the TOE workstation. Modification of audit logs and audit records are not allowed in maintaining the integrity of the audit logs as evidences of the operations of the TOE. TOE prevents any medication of audits logs and audit records on the TOE.

In the events of TOE operates after proper configuration applied upon the TOE, audit logs are enable once the TOE is running and operational. In general, TOE shall record all types of events relevant to TOE applicability based on Table 14. The segregation of information inside the logs is based on date, time, account user/s, event name, event types and more details, where applicable.

TOE Administrators may select the set of event to be audited. Only TOE Administrators can view the system logs. Logs cannot be deleted and modified from the database by anyone. In any cases of the log storage is full; the existing logs shall be overwritten and upon organizational security policy implemented to enforce any logs backup if needed. The system starts to overwrite the first log in order to store the incoming new logs.

Date and time data of the entire audit logs are received from a reliable NTP server relying from the underlying operating system, which is accepted as an extended security function.

TOE Security Functional Requirements Satisfied
FAU_GEN.3
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_STG.1
FAU_STG.4
FPT_STM.2

7.2 Authentication and Identification

To prevent unauthorized access to the TOE functions as well as reliable accountability for authorized TOE Administrator/s use of security functions, the SCAN S3 SMC require authorized TOE Administrator/s to perform authentication before they may access any of the TOE functions or data. Before authentication, the TOE Administrator/s will only see the login screen where information key in for login ID (Username/User ID), followed by the password/PIN with the enforcement ofPKI certificate types. All these been performed with the assistance of SCAN S3 AGENT, installed in the desktop. As for user/s that been enforced by the TOE information flow control policy, user/s will not have any access to the SCAN S3 SMC directly and only have access to protected resources bound by the TOE operations.

Each user/s and TOE Administrator/s shall be provided with minimum of one type of PKI component/tokenthat accessible using SCAN S3 AGENT installed in their desktop PC, for authentication and identification processes. At the access control web application login page, user/s shall provide all the components required and if the process successful, Staff (User) shall be allowed to access their dedicated resources. And if the process is unsuccessful, the error page of unsuccessful login process is not display or providing any detail information related to the event accordingly. This process is also applicable for TOE Administrator/s in accessing the SCAN S3 SMC.

The configuration of user/s access control, TOE Administrator/s shall comply with organization security policies. The Authentication module shall enforce users to re-authenticate when the sessions are expired.

Selection of PKI types shall configure by TOE Administrator/s. Process ofauthentication and identification shall performed verification process upon component submitted by user/s on login page; whilst validation of PKI towards the users are performed at the back-end system, which is the SCAN S3 SMC System.

TOE Security Functional Requirements Satisfied
FIA_ATD.1
FIA_UAU.2
FIA_UID.2
FIA_USB.1

7.3 Cryptography

Cryptographic operations are performed by the SCAN S3 AGENT on theuser/s desktop or workstation and alsoenforced at TOE Administrator/sworkstation or desktop, before processes of authentication and identification is been performed. Both of these categories are required to select their PKI type's token either using smart card, soft certificate, roaming certificate and applied it at SCAN S3 AGENT. These are been set by TOE Administrator/s based on organizational security policies implemented.

Furthermore, SCAN S3 AGENTalso perform import certificate, removecertificate, listing all certificates, capturing certificate from PKI token such as smart card, signing, verification, authentication, checking for roaming certificate for users of TOE in protection resources data transacted between user desktop browsers and TOE system. All resources are communicating and transacted securely based on this PKI implementation.

As for matter in usage of roaming certificate, SCAN S3 AGENTshall become software handler of the process of roaming certificate during authentication and identification processes, as well as, other cryptographic operations within the TOE boundary operations. SCAN S3 AGENTfor SCAN S3 SMC supports smart card, soft certificate and roaming certificate.

TOE Security Functional Requirements Satisfied
FCS_COP.1

7.4 Security Management

The TOE Administrator/sis applicable to configure the Security Management functions of the TOE within TOE Management function. The TOE Administrator/s can manage the user/s, access rights, managing accounts and PKI types within the Managementfunctions.

The TOE Administrator/s is authorized to perform the appropriate functions of creation, update and delete of information within the appropriate role boundary. The subject, object, operations and information that are related to TOE Administrator/s are stated in Table 12.

For initialization of SCAN S3 SMC, a default Login ID and soft certificate is provided to perform the creation of initial TOEAdministrator (Admin). The TOE Administrator (Admin) is responsible to create other administrator ID's and TOE users. The default login needs to be deleted by the new TOE Administrator. The new creation ID of TOE Administrator (Admin) shall be maintained as the main default account for the TOE, and shall not be deleted.

From the Management function, where TOE Administrator/s can review, perform auditing and editing configuration user/s preferences. The TOE Administrator/s may further segregate the user/s according to access rights and privileges.

The TOE Administrator (Admin)is able to create and delete other TOE Administrator/s, modify other TOE Administrator/s information and assign administrator roles appropriate. A single ID of an administrator can have only one role at a time. SCAN S3 SMC shall be maintained, configured and monitored by TOE Administrator/s. It is recommended to have minimum two (2) TOE Administrator/s (Admin), which is, one from the developer and one from the Headquarter (HQ).

Noted that, the initial creation of TOE Administrator with the role "Admin" are not recommended to be deleted and shall be assigned as default account TOE Administrator. Only TOE Administrator (Admin) account is allowed to delete other TOE Administrator/s (with same or lesser privileges) in the TOE.

To help in the operational level of the SCAN S3 SMC, TOE Administrator/s (Admin) shall assign more than one (1) TOE Administrator/s with less privileges and access rights. When there is inactivity of a user session for up to 20 minutes, the system will automatically prompt a reminder indicating session is almost expiring. User selects whether to end or proceed with the session. Upon ending the session, the user needs to re-login to access again. Thisis applicable for SCAN S3 SMC and also protected web resources.

TOE Security Functional Requirements Satisfied	
FTA_SSL.1	FDP_IFF.1
FMT_MOF.1	FDP_IFC.1
FMT_MTD.1	FIA_USB.1
FMT_SMF.1	
FMT_SMR.1	
FMT_MSA.1	
FMT_MSA.3	

7.5 User Data Protection

The TOE protects the all the resources internal assigned to be protected by TOE using access control enforcement by using information flow control. The TOE shall check and examined all mechanisms of authentication by all users with intention of access the protected resources by enforcing authentication and identification process. In accordance to access control policy and information flow control policy, all users shall require to provide legitimate and correct access control components such as username, password and PKI's. The decision to allow or reject/drop traffic access control will be based on configuration of access control configured by TOE Administrator/s.

TOE Administrator/s shall configure all access control policy based on information provided by organization policies and based on requirements set for certain protected resources.

By default, all access to the protected resources assigned is block by the TOE. Only assigned and legitimate TOE Administrator/shas the capabilities of setting the configuration of the TOE as assets of protecting information flow between users towards the protected resources including the TOE itself.

TOE Security Functional Requirements Satisfied
FDP_ACC.1
FDP_ACF.1
FDP_IFC.1

FDP_IFF.1

7.6 Protection of the TSF

The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment, which is, from the underlying operating system. NTP server is used as a reliable source of environment. However, NTP server itself is not part of the scope. TOE prevents manual modification of date and time to preserve integrity of date and time from NTP server.

TOE Security Functional Requirements Satisfied
FPT_STM.2

8 Rationale

8.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

8.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

8.2.1 Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.ACCESSLOG An unauthorized person successfully accesses the TOE data or security functions without being detected.	**O.ACCESSLOG** TOE shall record a readable log of security events.	This security objectives counter threat because any success or failure of authentication events will be recorded in a readable log of security events. Each security events will be audited or logged based on the compromised user ID presented by unauthorized person.
T.AUDIT An unauthorized person or authorized administrator may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.	**O.AUDIT** TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	This security objective counter threat because it will prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The objective also ensures the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
T.EXPLOIT An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.	**O.EXPLOIT** TOE shall mediate the information flow between users and web applications intended based on user requested.	This security objective counters threat because TOE will mediate the information flow between users and protected resources, whether to allow or drop information send by unauthorized person.
T.REMOTE An unauthorized person or	**OE.MGMT** The TOE shall be managed from	This security objective counters this threat because the deployment environment will

unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).	provides secure remote connection connectivity by administrator when remotely access the TOE. It also specifies that the TOE will be deployed in a separate network from the internal and external networks.
	OE.CONN Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters threat because the environment will provide a secure and encrypted connection to prevent unauthorized person or external IT entity sniffs the data and modifies it.
T.CONFIG An unauthorized person may read, modify, or destroy security critical TOE configuration data.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.	This security objective counters threat because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.
T.NOAUTH An unauthorized person may attempt to bypass the TOE access controls, in accordance to modify current existing security configurations, provided by the TOE.	**O.NOAUTH** The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective counters threat because security events are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. The audit records are not allowed to be modifies by administrator to preserve its integrity. Detection of bypassing actions through audit logs security enforcement enable TOE to capture the events and recorded it in the logs from TOE Administrator/s analysis and configure the TOE for better protections.
T.SPOOF	**O.EXPLOIT**	This security objective counters

An unauthorized person may carry out network spoofing and/or sniffing activities, in which, information flows through the TOE into a connected network by using a spoofed source address.	TOE shall mediate the information flow between users and web applications intended based on user requested.	threat because TOE will mediate the information flow between users and protected resources to decide whether to allow or drop information send by unauthorized person.

Table 15: Mapping Security Objectives to Threats

8.2.2 Rationale Security Objectives Mapped to OSP Rationale

OSP	Security Objectives	Rationale
P.ROLE Only authorized persons assigned by the organization have access to the TOE.	**OE.USER** Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	This security objective mapped back toOSP because unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.
	O.CONFIG TOE shall prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.	This security objective mapped back toOSP because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.
P.PASSWORD Authorized administrator shall use password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective mapped back toOSP because authorized administrator shall be non-hostile and follow guidance on creating a good password.

Table 16: Mapping Security Objectives to OSP

8.2.3 Rationale Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY The TOE and its environment are physically secure.	**OE.PHY** The TOE and its environment shall be physically secure.	This security objective mapped back to assumption because the TOE and its environment shall be physically secure.
	OE.SOFTCERT Authorized TOE Administrator/s shall be able to keep and secure the soft certificates in the secure location (logically or physicaly) and performed regular backup of those soft certificates.	This security objective mapped back to assumption because the TOE and its environment in providing a secure operational environment in safekeeping the soft certificates.
A.FLOW Information cannot flow through internal and external networks unless it passes through the TOE.	**OE.FLOW** The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.	This security objective mapped back to assumption becauseTOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
A.ADMIN Authorized administrators are non-hostile and follow guidance; however, they are not free from error.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective mapped back to assumptionbecauseauthorized administrators shall be non-hostile and follow guidance; however, they are not free from error.
A.TIMEBACK The TOE environment will provide reliable time stamps and backup storage enough for TOE supporting operational environments.	**OE.TIMEBACK** The TOE environment shall provide reliable time stampsand backup storage enough for TOE supporting operational environments.	This security objective mapped back to assumption becauseTOE environment shall provide reliable timestamps and backup storage.
A.MGMT The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only	**OE.MGMT** The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only	This security objective mapped back to assumption because TOE shall be managed from a network that is physically separated from the internal and external networks. Remote

permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN).	permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).	management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).
A.CONN Authorized administrators will access the TOE using a secure connection.	**OE.CONN** Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective mapped back to assumption because authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.
A.USER Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	**OE.USER** Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	This security objective mapped back to assumption because unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.

Table 17: Mapping between Security Objectives and Assumptions

8.3 Extended Security Functional Requirement Rationale

Refer Section Extended Security Functional Requirement (SFR) for the rationale.

8.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

8.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

8.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Table 18: Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.ACCESSLOG TOE shall record a readable log of security events.	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_SAR.1	This SFR specify that administrator will have the capability to view the audit trail data in log form. It traces back to this objective.
	FAU_SAR.2	This SFR specify that administrator will have the ability to select log file related to the security event. Administrator is able to filter the log for a better view. It traces back to this objective.
O.AUDIT TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by administrator or unauthorized person. It traces back to this objective.
	FAU_STG.4	This SFR specify that if the log file reach the size limit, TOE will create a new log file to ensure that the integrity of audit records is preserved. Audit records will not be appended. It traces back to this objective.
	FPT_STM.2	This SFR specify that the environment (NTP server) will provide a reliable time stamps for TOE, thus preserving the integrity of the security event date and time that is being audited. It traces back to this objective.
O.EXPLOIT TOE shall mediate the information flow between users and web applications	FDP_IFC.1	This SFR identify the external IT entities in the Unauthenticated Information Flow Control SFP that send information to other entity. The SFP will either reject or allow the information flow. It traces back to this

intended based on user requested.		objective.
	FDP_IFF.1	This SFR identify the external IT entity and its security attributes as part of the information flow control SFP. TOE will permit or deny the information flow through the TOE based on access control policy configured by TOE Administrators. It traces back to this objective.
O.CONFIG	FDP_ACC.1	This SFR provide users with attributes to

	FDP_ACF.1	
	FIA_ATD.1	This SFR provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_USB.1	This SFR enforce each user bind with specific components such as TOE in fulfilling access control requirements. Therefore, unauthorized person will require longer duration and higher processing speed to guess/brute force the OTP (One Time Password) in order to be authenticated. It traces back to this objective.
	FMT_MOF.1	This SFR restrict the ability to enable, disable and modify TOE functions to administrator. It traces back to this objective.
	FMT_MTD.1	This SFR restrict the ability to change default value, modify, delete and add user attributes in FIA_ATD.1.1 to administrator. It traces back to this objective.
	FMT_SMF.1	This SFR identify management functions that are available in TOE as in FMT_MOF.1.1, that are managed by administrator. It traces back to this objective.
	FMT_SMR.1	This SFR identify the roles exist in TOE, which is TOE Administrators. Each user account created must be associated to administrator role that have access to TOE management interface. It traces back to this

		objective.
	FMT_MSA.1	This SFR restrict the ability to change default value, modify, delete and add subject and information security attributes in access control policy, as in FDP_IFF.1.1 to administrator. It traces back to this objective.
	FMT_MSA.3	This SFR enforce a restrictive access control protection by default (during the initial start of TOE). Administrator will have access to management interface to modify the default value in access control. It traces back to this objective.
O.NOAUTH The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	FCS_COP.1	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. In this requirements stated the enforcement of OTP usage and verifications on the OTP generated.It traces back to this objective.
	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.Detection of bypassing actions through audit logs security enforcement enable TOE to capture the events and recorded it in the logs from TOE Administrator/s analysis and configure the TOE for better protections.
	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by administrator or unauthorized person. It traces back to this objective.Detection of bypassing actions through audit logs security enforcement enable TOE to capture the events and recorded it in the logs from TOE Administrator/s analysis and configure the TOE for better protections.
	FAU_STG.4	This SFR specify that if the log file reach the size limit, TOE will create a new log file to

		ensure that the integrity of audit records is preserved. Audit records will not be overwritten. It traces back to this objective.Detection of bypassing actions through audit logs security enforcement enable TOE to capture the events and recorded it in the logs from TOE Administrator/s analysis and configure the TOE for better protections.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a basic assurance. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of basic.

END OF DOCUMENT