Nexbis Sdn. Bhd.

NexCode National Security Suite
Release 3

Security Target
Version 8.4

20th May 2011

DOCUMENT HISTORY

Version Number	Version Date	Change Details
0.1	13-10-2009	Initial draft.
0.2	19-11-2009	Revised copy.
0.3	20-11-2009	Replaced image, numbered table and rearranged indentation.
0.4	23-12-2009	Minor updates.
1.0	23-12-2009	Updated physical diagram.
2.0	13-01-2010	Overall updates.
3.0	22-01-2010	Overall revision.
4.0	08-02-2010	Overall revision based on latest ERR1-d1b and ERR2-d1.
4.1	22-03-2010	- Transfer of ST authorship to Drexx Laggui <Drexx@Laggui.com> from Juliet Looi. - Edited minor typographical errors. - Added A.TIME and OE.TIME to satisfy FPT_STM.1
5.0	23-03-2010	Minor updates on the following: o Overall document formatting; o Table of contents; o Replaced figure 4.
6.0	23-04-2010	Minor updates on the following: o Edited Section 2.2.1 as per advice; o Updated with Section 2.2.2; o Fixed various numbering and formatting issues; o Inserted the word "consecutive" in the description for ITSF.RETRY.FAIL; o Removed all instances and references to FIA_UAU.1; o Corrected dependencies for FCS_COP.1(2):MD5 and FCS_COP.1(3):VeriSign; o Updated ST for compliance to document conventions for SFRs; o Clarified ITSF.RETRY_FAIL in TSS; o Clarified rationale for FIA_UID.2; o Edited T.SYS_FAIL to clarify threat agent in statement; o Standardized Table 4 as per advice.
7.0	16-06-2010	- Transfer of authorship from Drexx Laggui to Michael Dalud (michael.dalud@laggui.com)

		- Updates on the following: o Changed ST Title in section 2.1 (ST and TOE Reference) to correspond with Front Page Title. o Identified TOE as a software system in Section 2.1 (TOE Overview) to correspond with Section 2.2.1 (TOE Type). o Re-wrote TOE Overview text o Removed text highlighting (boldface) to avoid confusion. o Edited paragraphs to be more understandable to consumers. o Specified the location of the list of hardware, software, and guidance parts that constitute the TOE. o Edited and highlighted (boldface) text to clarify that the areas surrounded by the dashed lines represent the physical scope of the TOE. o Security function descriptions have been integrated into corresponding TOE scope descriptions. o Edited section 2.3.1.1. o Omitted lengthy explanations as per evaluator's advice. o P.FAIL_HD removed due to the reduced scope of the TOE. o OE.PHYST integrated into OE.PHYSEC as recommended by evaluator. o O.FAILOVER removed due to the reduced scope of the TOE. o Effects on threats and policies are now specified for each claim. o T.SYS_FAIL removed due to the reduced scope of the TOE. o OE.FAILHD removed due to the reduced scope of the TOE.
8.0	30-06-2010	o Edited paragraphs in Section 2.3.1.2 to focus only on descriptions of TOE components o Added FCS_CKM.1 and FCS_CKM.4 to Section on Toe Security Functional Requirements and to Table 7 o Edited Section 8 for clarity and consistency. o Edited Section on SFR Dependency Rationale (Table 12) for clarity on unsatisfied dependencies o Added “checksum” to Terminologies section
8.1	23-07-2010	o Edited FCS_CKM.1(1) and FCS_CKM.4(1) to FCS_CKM.1 and FCS_CKM.4 respectively o Edited FCS_COP.1, FCS_COP.2 and FCS_COP.3 following CR_001 from MyCB o Removed ‘marketing words’ as mentioned in CR_001 from MyCB from TOE Overview.
8.2	23-08-2010	Made the following amendment:-

		o Deleted the word ‘innovative’ in the first paragraph of TOE Overview. o Removed ‘is designed to address the over increasing need’ from the second paragraph of TOE Overview. o Updated the term ‘different departments’ to ‘external verification database’ of TOE Type. o Removed clustered server implementation from all relevant sections:- 2.3.1.1 (Figure 1 and text) and 2.3.1.2 (Figure 2, text, Table 2(1), Table 2(2) and Table 3). o Changed section 2.3.1.3 to follow the Preparative procedure and Operational procedure file names. o Under section 7.2, edited the term to ‘user password’ instead. The term ‘administrative user password’ basically refers to a password generated during when an administrator creates a user account using the TOE. It has nothing really much relate to the type of user. o Under section 7.2, edited the term ‘administrative user’ to ‘administrator’. Is FMT_SMR necessary to include? o Under section 7.2, amended ‘TSF data’ to ‘TOE data’ instead. Inserted an application notes to indicate the meaning of the term ‘TOE data’. o Under section 7.2, edited the term ‘administrative user’ to ‘administrator’ since ultimately the term is referring to an administrator. o Under section 7.2, expanded the audit information to ‘all audit information (login, logout, view, search, add, update, delete and its timestamp)’ o Under section 7.2, changed the configurable inactivity to the following phrase:- [15 minutes by default or other specified time interval of user inactivity set by an authorized administrator] instead. o Under section 7.2, changed the term 'AES PRNG’ to its fuller term ‘AES Pseudorandom Number Generator’ instead. The term is

		referring to the algorithm used in the cryptography for generating a sequence of numbers that approximates the properties of random numbers. o Under section 7.2, modified to change to 'AES cryptographic key destruction' with standard as 'FIPS 197 (AES)' instead. o Under section 7.2, appended application note as stated. o Added back section renumbering to every parts of document. o Added 'Cryptographic key management (FCS_CKM)' family to Table 5 under section 7.1.
8.3	25-04-2011	Made several changes based on feedback from evaluators on the last round of progress meeting with Cybersecurity (20/10/2010):- o Amended section 2.3.1.4 "Logical Scope of the TOE" description under security function "Identification and Authentication" to only mention TOE instead of specifying the items. o Updated section 7.2.1 - "FIA_ATD.1" to include group role and rights. o
8.4	20-05-2011	Removed FCS_COP.1(2) MD5 and all references to it (TSF, Security Objective, threat mappings and FTP_TRP.1 and all references to it.

Table of Contents

1 DOCUMENT INTRODUCTION

1.1 DOCUMENT CONVENTIONS

The following conventions have been applied in this document:
Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.
1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underlined text**. Refinement for taking out a security requirement within the SFR's is denoted by ~~**bold strikethrough text**~~ in red color font.
2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*].
3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

1.2 TERMINOLOGIES

Table 1: Terminologies and Meanings

Terminology	Meaning
CC	Common Criteria
FIPS PUB	Federal Information Processing Standards Publication
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

TSS	TOE Summary Specification
auditor	a person appointed to collect and evaluate evidence of an organization's information systems, practices, and operations; the evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.
checksum	also known as hash value or hash sum, is a value derived from the bits of a block of digital data that is calculated before and after transmission or storage to gain assurance that the data is free from errors or tampering
diminish	to reduce or lessen
mitigate	to make less severe or less harsh
system administrator	a person employed to maintain and operate a computer system and/or network.

1.3 REFERENCES

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

1.4 DOCUMENT ORGANIZATION

This ST contains:

- TOE Description: Provides an overview of the TOE and describes the physical and logical scope for the TOE
- TOE Security Problem Definition: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- TOE Security Objectives: Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- TOE Security Functional Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE
- TOE Security Assurance Requirement: Presents the Security Assurance Requirements (SARs) met by the TOE
- TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives
- Rationale: Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability

2 INTRODUCTION

2.1 ST AND TOE REFERENCE

ST Title	*NexCode National Security Suite, Release 3 - Security Target*
ST Version	*Version 8.4, 20th May 2011*
TOE Identification	*NexCode National Security Suite, Release 3*
CC Identification	*Common Criteria version 3.1*
Assurance Level	*EAL2*
ST Author	*Michael Dalud*
Keyword	*TOE*

2.2 TOE OVERVIEW

The target of evaluation is the NexCode National Security Suite, a software system that utilizes mobile telephone technology with real-time information access to enhance the security of identification and authentication of documents. Using NexCode, a proprietary 2D barcode, the NexCode National Security Suite provides real-time information access and information sharing using standard camera-enabled mobile phones, and is secured with encryption. The user scans the NexCode printed on an individual's identification document (even photocopied documents) via a mobile phone equipped with NexCode software to verify the information against the centralized source data. This source is cross-linked to other databases, enabling accuracy of a person's identification. Every transaction takes only seconds and is updated in the system reports.

The NexCode National Security Suite is for fast and reliable identity authentication, document security, fraud detection, and various other scenarios requiring identification enforcement.

The TOE has multiple components, each having a distinct function. These components are:

- The NexCode Inventory System – for generating NexCode barcodes and ensuring secure transfer of generated NexCode barcode images into the NexCode Load System;
- The NexCode Load System – for managing successfully transferred inventory load files for the NexCode Control Centre System;
- The NexCode Control Centre System – for managing user and group access control and operation configuration;
- The NexCode Gateway System – for managing secure communication with the mobile client or the desktop client;
- The NexCode Mobile Application – for scanning and decoding Nexcode barcodes through mobile phones.
- The NexCode Desktop Application – for scanning and decoding Nexcode barcodes through desktop computers.

The security functions provided by the TOE include the following:

Identification and Authentication:

- Login and user group identification and authentication implemented with unique username and authenticated password having access rights controlled by the user group
- User login blocked after three attempts of incorrect password in accessing NexCode Control Centre System

Cryptographic Support

- Use of AES encryption in securing communications channels between the TOE Gateway Server and the mobile client or the desktop client
- The NexCode Mobile Application is signed and verified using VeriSign

Security Audit Data Generation

- Audit trail and logging on the NexCode Control Centre System, the NexCode Mobile Application and the NexCode Desktop Application

Protection of the TOE Security Functions

- Use of Secure FTP (SFTP) to secure data transfer of TOE inventory files composed of NexCode 2D barcode images from the TOE Inventory Server to the TOE Load Server

TOE Access

- User session idle time-out within the NexCode Control Centre Web application upon a configured idle time.

2.2.1 TOE Type

This TOE is the **NexCode National Security Suite**, a software system for cross-referencing of information for enforcement and authentication needs. Due to its currently unique nature and operation, its type is further described below:

Using a Webcam or a standard camera-equipped mobile phone, the user can scan identification documents that have a proprietary barcode, called *Nexcode*, printed on them. The NexCode National Security Suite can then be used to request information regarding authenticity, validity, and identity.

Requests for information are transacted in real-time from the external verification database, and the NexCode National Security Suite ensures that accurate and valid information is given to the user within only a few seconds after the request. For security, sending and receiving of data is done over encrypted connections.

The user is required to log in with the appropriate user name and password to use the system. The NexCode National Security Suite determines the level of access to privileged information according to the user's identity.

For audit purposes and accountability, user actions using the NexCode National Security Suite are recorded. To aid in management, built-in reporting tools facilitate the viewing of usage and performance information.

2.2.2 Required non-TOE hardware, software, or firmware

The TOE is a software product that is installed on an AMD or Intel-based CPU hardware platform, in combination with an operating system (OS) and 3rd-party software applications. Details are expanded in Section 2.3.1.

The operating system platforms supported are:

- Microsoft® Windows® 2003 Server (standard and enterprise editions)
- openSUSE Linux version 10.2

The required 3rd-party application systems include:

- Apache Tomcat version 6.0.14
- Java ME with MIDP 2.0 or above and CLDC 1.1 or above
- Java Media Framework 2.1
- Java Runtime Environment 6.0
- Java SDK version 1.5.0.11
- JBoss application server version 4.2.3
- Jetty web server version 6.1.22
- MS Internet Explorer 7.0 / 8.0
- MySQL version 5.0.27

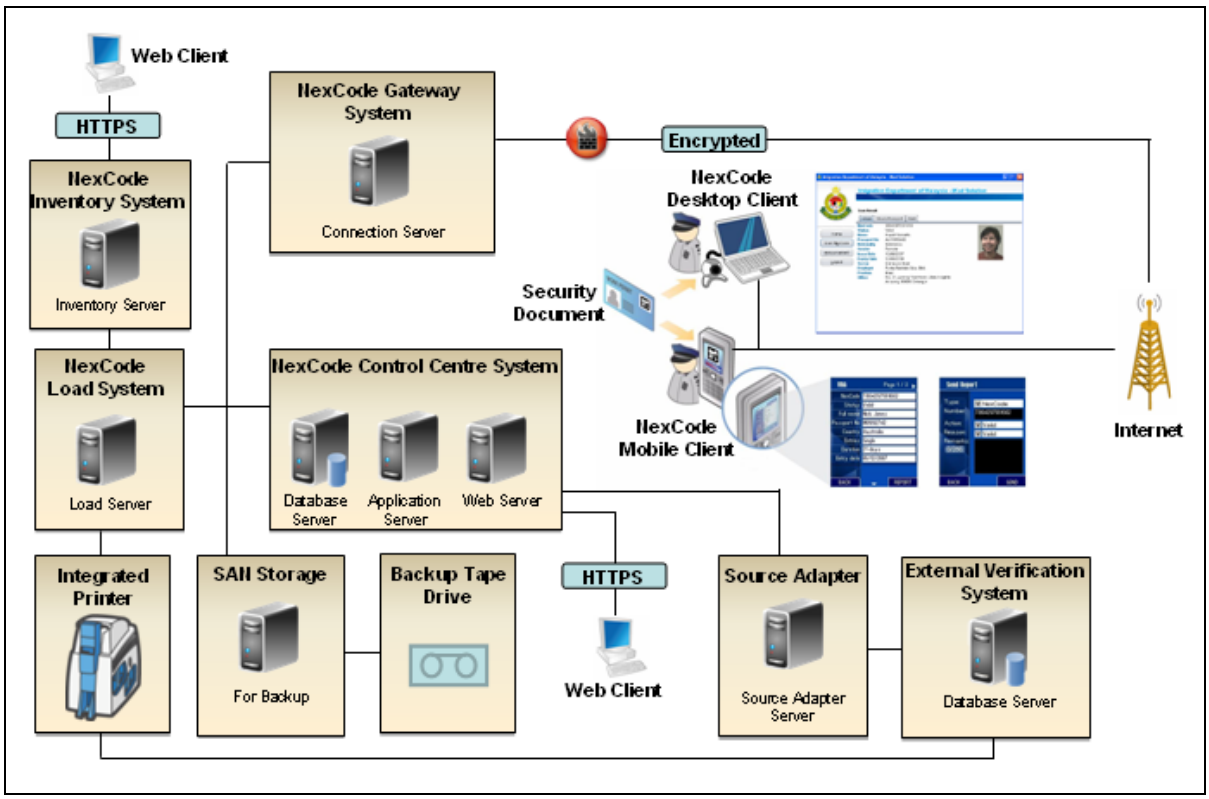
2.3 TOE DESCRIPTION

2.3.1 Physical Scope of the TOE

The following subsections describe the operational environment of the NexCode National Security Suite, physical scope of the TOE, and the relevant hardware or software structures.

2.3.1.1 Operational Environment of the NexCode National Security Suite

Figure 1: Operational Environment of the NexCode National Security Suite

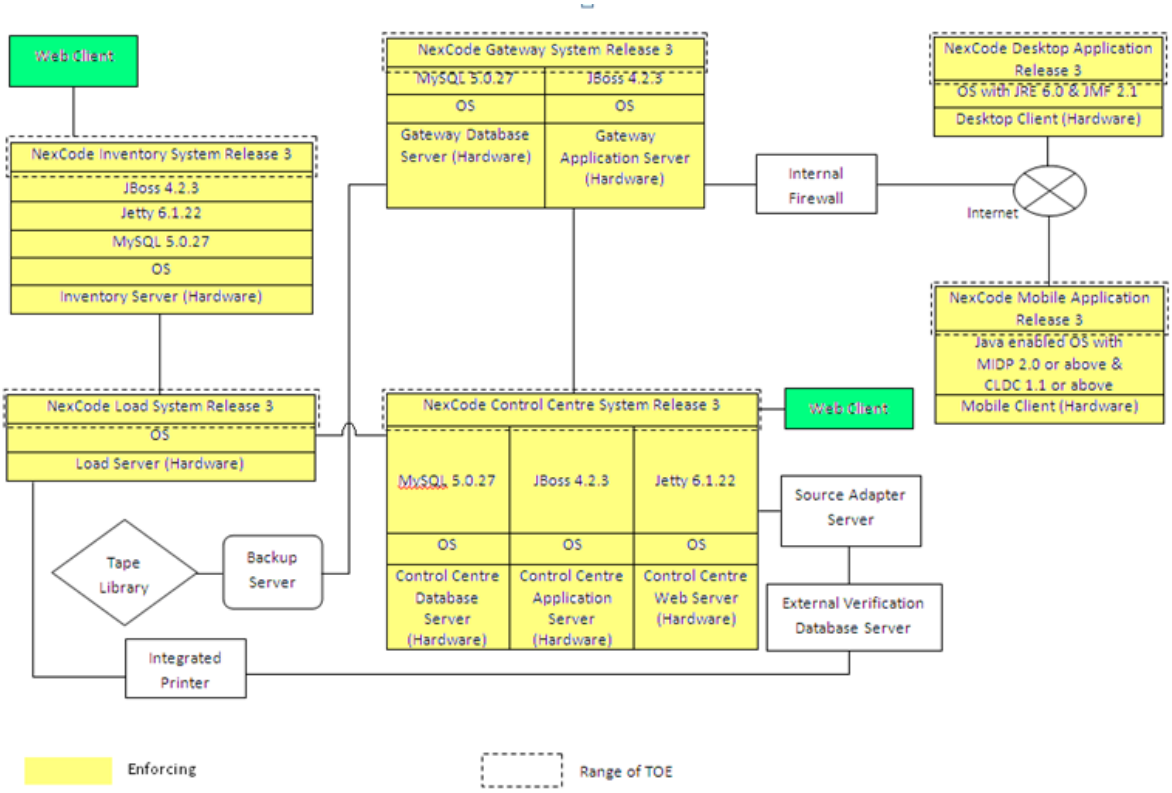


The hardware, software, and guidance parts that constitute the TOE are enumerated in the tables in Sections 2.3.1.2 and 2.3.1.3. There are no firmware parts for the TOE.

2.3.1.2 Physical Scope of the TOE (Components)

The areas surrounded by the dashed lines represent the physical scope of the TOE (the NexCode National Security Suite) in *Figure 2.* Details for each component are provided in the paragraphs following the figure.

Figure 2: Physical Scope of the NexCode National Security Suite (areas surrounded by dashed lines)



- The NexCode Inventory System manages generation of TOE inventory files (NexCode 2D barcode images) and inventory reports. The TOE application server (JBoss 4.2.3), the TOE Web server (Jetty 6.1.22) and the TOE database server (MySQL 5.0.27) all reside in a single physical server named Inventory Server.

- The NexCode Load System handles inventory loading and stores the TOE inventory files for the NexCode Control Centre System. The Load Server manages storage and reference of TOE inventory files in a single physical server through UNIX-based scripts.

- The NexCode Control Centre System manages the TOE inventory files in the Load Server, and handles the encryption of user passwords before they are stored into the database.

  The NexCode Control Centre System is the component of the TOE that provides users with a Web application front-end for log-in, as well as for administration and configuration functions. Through this front-end, authorized users can also read various TOE user log reports in order to monitor and audit the usage of the TOE system.

The log information used for reporting and audit trails is stored within a database in the Control Centre Database server.

The non-TOE External Verification Database Server is the source database from where data request is retrieved via the Source Adapter Server connected to the NexCode Control Centre System.

- The NexCode Gateway System handles data encryption, routing and connection between the gateway with the mobile client or the desktop client.
- The NexCode Mobile Application handles mobile user functionality, scanning, and decoding through the mobile client.
- The NexCode Desktop Application handles desktop user functionality, scanning, and decoding through the desktop client.

The non-TOE Backup Server and non-TOE Tape Library storage device both handle periodic data backup on TOE NexCode Gateway Database Server and TOE Control Centre Database Server, including files backed up from the TOE Load Server. Data and files from each TOE server are first backed up to the Backup Server before outputting to a tape library as an external storage.

The non-TOE Integrated Printer handles printing of the NexCode 2D barcode image onto each security document with a unique serial number.

The software configuration of the TOE is shown in *Table 2*. The TOE will operate correctly and reliably in the software configuration identified in the table.

Table 2(1): Software Configuration of the TOE

Equipment Name	**Vendor Name**	**Product Name**	**Type**
Inventory Server	Nexbis	NexCode National Security Suite – Inventory Management Release 3	Back-end core and front-end web application software
Load Server	Nexbis	NexCode National Security Suite – Load Server Release 3	Application scripting software
Control Centre Web Server	Nexbis	NexCode National Security Suite – Control Centre Release 3 (Web)	Front-end web application software
Control Centre Application Server	Nexbis	NexCode National Security Suite – Control Centre Release 3 (Core)	Back-end core application software
Gateway Application Server	Nexbis	NexCode National Security Suite – Gateway Server Release 3 (Core)	Back-end core application software
Desktop Client	Nexbis	NexCode National Security Suite – Desktop Application Release 3	Desktop application software

Mobile Client	Nexbis	NexCode National Security Suite – Mobile Application Release 3	Mobile application software

Table 2(2): Software Configuration, non-TOE

Equipment Name	**Vendor Name**	**Product Name**	**Type**
Inventory Server	JBoss	JBoss application server version 4.2.3	Application server
	Jetty	Jetty web server version 6.1.22	Web server
	Microsoft	I.E 7.0	Web browser
	Sun Microsystems	MySQL version 5.0.27	Database
	Linux	openSUSE Linux version 10.2	Operating system
	Sun Microsystems	Java SDK version 1.5.0.11	System Development Kit

Load Server	Linux	openSUSE Linux version 10.2	Operating system
Control Centre Web Server	Jetty	Jetty web server version 6.1.22	Web server
	Microsoft	I.E 7.0	Web browser
	Linux	openSUSE Linux 10.2	Operating system
	Sun Microsystems	Java SDK version 1.5.0.11	System Development Kit
	Sun Microsystems	MySQL version 5.0.27	Database
Control Centre Application Server	JBoss	JBoss application server version 4.2.3	Application server
	Linux	openSUSE Linux 10.2	Operating system

	Sun Microsystems	Java SDK version 1.5.0.11	System Development Kit
Control Centre Database Server	Sun Microsystems	MySQL version 5.0.27	Database
	Linux	openSUSE Linux 10.2	Operating system
Gateway Application Server	JBoss	JBoss application server version 4.2.3	Application server
	Linux	openSUSE Linux 10.2	Operating system
	Sun Microsystems	Java SDK version 1.5.0.11	System Development Kit
Gateway Database Server	Sun Microsystems	MySQL version 5.0.27	Database
	Linux	openSUSE Linux 10.2	Operating system

Desktop Client	Sun Microsystems	Java Runtime Environment 6.0	Java virtual machine and library
	Sun Microsystems	Java Media Framework 2.1	Java library
Mobile Client	Sun Microsystems	Java ME with MIDP 2.0 and CLDC 1.1	Device platform

Table 3 below shows the hardware configuration of the TOE of which the TOE will operate correctly and reliably in the hardware configuration identified in the table.

Table 3: Hardware Configuration of the TOE

Server	**Specifications**	**Description**
Inventory Server	Processor	1x Intel Quad-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1 & 3TB SAN Storage
Load Server	Processor	1x Intel Dual-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1 & 1TB SAN Storage
Control Centre Web Server	Processor	1x Intel Quad-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1
Control Centre Application Servers	Processor	2x Intel Quad-Core Xeon 3Ghz
	Memory	32 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1
Control Centre Database Server	Processor	2x Intel Dual-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1 & 1TB SAN Storage
Gateway Application Server	Processor	1x Intel Quad-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1
Gateway Database Server	Processor	1x Intel Dual-Core Xeon 3Ghz
	Memory	16 GB RAM
	Disk Drive	2x 146GB SAS 15K RAID1

Desktop Client	Processor	1x Intel Duo Core 2.7Ghz
	Memory	2 GB RAM
	Disk Drive	160GB
	Camera	Web Cam
Mobile Client	Screen	128x160 Pixels
	CLDC	v1.1
	MIDP	v2.0
	JSR Support	JSR-135 (Mobile Media API) for image scanning
	Camera	VGA
	Memory	250 kbytes
	Data Access	GPRS/3G/EDGE

2.3.1.3 Physical Scope of the TOE (Guidance)

The following TOE guidance manuals are provided:

- Preparative Procedure – “Nexbis-NSS-r3_AGD-PRE_EAL2_ver1.1.doc”
- Operational User Guidance – “Nexbis-NSS-r3_AGD-OPE_EAL2_ver1.1.doc”

2.3.1.4 Logical Scope of the TOE

The TOE scope description on each TOE security function is summarized in *Table 4* below. Each TOE security function is categorized according to its functional requirement class.

Table 4: TOE Security Function map to TOE Scope

Security Function	**TOE Scope Description**
Identification and Authentication	
ITSF.I&AUT	TOE user and group access control: TOE user with unique username is authenticated by password with access rights controlled by either an individual user or a user group within the TOE.
ITSF.RETRY_FAIL	Three times authentication failure: TOE user login is blocked upon three consecutive attempts of incorrect password entry in accessing NexCode Control Centre System.
Cryptographic Support	
ITSF.ENCRY_DAT	Encrypted communication channel between TOE Gateway Server and enforcement tools: Data transferred between the TOE Gateway Server and the mobile client or the desktop client is encrypted using AES encryption.
ITSF.SIGN_MOB	Trusted TOE mobile application: The TOE Mobile Application installed on the mobile client is signed and verified.
Security Audit Data Generation	
ITSF.AT&L	Audit trail and logging: The following applies to NexCode Control Centre System web application, the NexCode Mobile Application and the NexCode Desktop Application: o All TOE user access login or logout is logged and auditable; o All action taken against any TOE data is logged and auditable. o The IT Environment is relied on to provide reliable time stamps for use in collected audit data. Collected audit data are stored in files in the IT Environment, which the TOE relies on to protect as well.

Protection of the TOE Security Function	
ITSF.SEC_DATA	Secure FTP on transferring TOE inventory files: Usage of Secure FTP (SFTP) to transfer generated TOE inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server.
TOE Access	
ITSF.TIMEOUT	Login session idle time-out: The TOE user login session is timed-out within NexCode Control Centre System web application upon a configured idle time (default 15 minutes) to prevent unauthorized TOE users from accessing it.

3 CONFORMANCE CLAIMS

3.1 COMMON CRITERIA CLAIMS

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

- **CCv3.1 Rev.3 conformant**. The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 3;
- **Part 2 conformant**. The ST is Common Criteria Part 2 conformant;
- **Part 3 conformant**. The ST is Common Criteria Part 3 conformant;
- **Package conformant**. The ST is package conformant to the package Evaluation Assurance Level EAL2;
- **Protection Profile conformance**. The ST claims conformance to the following Protection Profiles: **None.**

4 TOE SECURITY PROBLEM DEFINITION

4.1 ASSUMPTION

This section describes assumptions that are applied to the TOE and its operational environment.

1. **A.PHY_ACC (physical access)**

   Accessing to data centre and servers kept on server rack requires only authorized personnel and system authentication.

2. **A.TIME (correct time)**

   The TOE operating environment will provide reliable system time.

4.2 THREATS

This section describes the assets protected by the TOE and the threats.

4.2.1 Assets Protected by the TOE

Types of user data, assets to be protected by the TOE listed are:- system access control data, the inventory generation data, enforcement configuration data, mobile client or the desktop client enforcement data, gateway communication data and reporting data.

4.2.2 Threats against the TOE

This section describes threats against the TOE.

1. **T.ILLEGAL_ACCESS (illegal access)**

   An authorized TOE user with administrator privileges may destroy or disclose any data or perform operations that are not authorized for each user role such as the following:

   - Creating, updating or deleting of inventory generation records;
   - Creating, updating or deleting of enforcement and operation records;
   - Registering, updating or deleting existing user or group privileges;
   - Creating and assigning of new user or group and its privileges;
   - Viewing of data from reports on inventory, operational and enforcement activities.

2. **T. DATA_INTERCEPT (data interception)**

Experienced hackers may maliciously listen and tamper:

- The data along the communication channel between NexCode Gateway Server and the enforcement tools (the mobile client or the desktop client);
- The files transferred from the NexCode Inventory Server to the NexCode Load Server;
- The HTTP request for any web client accessing NexCode Control Centre System.

3. **T. BYPASS (authentication bypass)**

Unauthorized person may successfully violate the authenticity of rules by succeeding to bypass the authentication.

4. **T. UNTRUSTED_APP (untrusted application)**

User may be accessing an un-trusted application which is not signed and verified.

4.3 ORGANIZATIONAL SECURITY POLICIES

This section describes organizational security policies that are applied to the TOE and its operational environment.

1. **P.ADMIN_IDENTIFY (identification of an administrator)**

Authorized System Administrator and the Auditor who use the TOE are subject to the TOE identification to keep a record of TOE access logs.

2. **P. AUDIT_LOG (audit logs)**

The ability to access the TOE audit logs is be restricted to the Auditor only in order to track unauthorized operations on the TOE assets to be protected.

5 TOE SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVE FOR THE TOE

This section defines the IT security objectives that are to be satisfied by the TOE in combination with the IT security environment. *Table 10* in *section 7.4.2* correlates the TOE security objectives to each of the threats and security policies, showing that each threat is countered by at least one IT security objective, and that each security policy is satisfied by at least one IT security objective.

1. **O.I&A**

   The TOE must provide login and user identification and authentication by allowing only authorized username and authenticated password to gain access to the system having access rights controlled by either an individual user or a user group.

2. **O. AUDIT_LOG**

   The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to trace user activities within the system.

3. **O. LOGIN_FAIL**

   The TOE must prevent or block users to login to the system after three attempts of incorrect password.

4. **O. ENCRYPT_DATA**

   The TOE must ensure that the data along communication channel between the NexCode Gateway Server and the enforcement tools (the mobile client or the desktop client) is encrypted using AES encryption.

5. **O. SECURE_DATA**

   The TOE must ensure that the inventory files (NexCode 2D barcode images) transferred from the NexCode Inventory Server to the NexCode Load Server is via the Secure FTP (SFTP).

6. **O.SIGN_MOB**

   The TOE must ensure that the NexCode Mobile Application is signed and verified using Verisign.

7. O. TIMEOUT

The TOE must ensure that the user access to the system is timed-out after a period of defined idle time.

5.2 SECURITY OBJECTIVE FOR THE ENVIRONMENT

1. OE.PHYSEC

The TOE operating environment must ensure that the TOE is physically secured and located within a secure controlled access facility i.e. data centre, which will prevent unauthorized physical access or modification.

2. OE.TIME

The TOE operating environment must provide a reliable time source for the TOE to provide accurate timestamps for audit records.

6 EXTENDED COMPONENTS DEFINITION

<This section is not applicable. There is no extended component.>

7 IT SECURITY REQUIREMENTS

7.1 OVERVIEW

Table 5: SFR map to Class, Family and Component

Class	Family	Component	SFR
Identification and Authentication (FIA)	User attribute definition (FIA_ATD)	User attribute definition (FIA_ATD.1)	FIA_ATD.1.1
	Authentication failures (FIA_AFL)	Authentication failure handling (FIA_AFL.1)	FIA_AFL.1.1
			FIA_AFL.1.2
	User identification (FIA_UID)	User identification before any action (FIA_UID.2)	FIA_UID.2.1
	User authentication (FIA_UAU)	User authentication before any action (FIA_UAU.2)	FIA_UAU.2.1
Security Audit Data Generation (FAU)	Security audit data generation (FAU_GEN)	Audit data generation (FAU_GEN.1)	FAU_GEN.1.1
		User identity association (FAU_GEN.2)	FAU_GEN.2.1
	Security audit review (FAU_SAR)	Audit review (FAU_SAR.1)	FAU_SAR.1.1
			FAU_SAR.1.2
		Restricted audit review (FAU_SAR.2)	FAU_SAR.2.1
		Select able audit review (FAU_SAR.3)	FAU_SAR.3.1
	Security audit event storage (FAU_STG)	Protected audit trail storage (FAU_STG.1)	FAU_STG.1.1
			FAU_STG.1.2
TOE Access (FTA)	Session locking and termination (FTA_SSL)	TSF-initiated termination (FTA_SSL.3)	FTA_SSL.3.1
Cryptographic Support (FCS)	Cryptographic operation (FCS_COP)	Cryptographic Operation (FCS_COP.1)	FCS_COP.1.1
	Cryptographic key management (FCS_CKM)	Cryptographic Key Generation (FCS_CKM.1)	FCS_CKM.1.1
		Cryptographic Key Destruction (FCS_CKM.4)	FCS_CKM.4.1
Protection of the TSF (FPT)	Internal TOE TSF data transfer (FPT_ITT)	Basic internal TSF data transfer protection (FPT_ITT.1)	FPT_ITT.1.1
	Time stamps (FPT_STM)	Reliable time stamps (FPT_STM.1)	FPT_STM.1.1

7.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

7.2.1 FIA Identification and authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [account name, group role, user role, group rights, user rights and user password].

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of identification

FIA_AFL.1.1 The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [user log in authentication to any application within the system].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [disable the user until unlocked by an administrator].

FIA_UID.2 User identification before any action

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

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.2 FAU Security audit data generation

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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 [*basic*] level of audit; and
c) [Each user login and logout actidon and any user action (add, update, delete, search and view) taken against any TOE data].

Application Notes: The term 'TOE data' refers to data that is generated or used within the target of evaluation.

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 ST, [None].

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 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.

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [an administrator who is authorized to read audit records] with the capability to read [all audit information (login, logout, view, search, add, update, delete and its timestamp)] 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.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.
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.

FAU_SAR.3 Select able audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [searches] of audit data based on [account name and / or date].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.
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.

7.2.3 FTA TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [15 minutes by default or other specified time interval of user inactivity set by an authorized administrator].

7.2.4 FCS Cryptographic Support

FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction]

FCS_CKM.1: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES Pseudorandom Number Generator] and specified cryptographic key sizes [128, 192 and 256 bits] that meet the following: [FIPS 197 (AES)].

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.
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: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [AES cryptographic key destruction] that meets the following: [FIPS 197 (AES)].

FCS_COP.1(1) Cryptographic Operation (AES)

Hierarchical to: No other components.
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(1) The TSF shall perform [encryption on data communicated between the NexCode Gateway Server and the mobile client or the desktop client] in accordance with a specified cryptographic algorithm [AES, Advanced Encryption Standard] and cryptographic key sizes [128, 192 and 256 bits] that meet the following: [FIPS 197 (AES)].

FCS_COP.1(2) Cryptographic Operation (Verisign)

Hierarchical to: No other components.
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(2) The TSF shall perform [signing and verification on the NexCode Mobile Application] in accordance with a specified cryptographic algorithm [SHA1-RSA] and cryptographic key sizes [1024 bits] that meet the following: [FIPS PUB 186].

7.2.5 FPT Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: This SFR ensures that the TOE obtains accurate time from the underlying operating system in the TOE environment.

7.3 TOE SECURITY ASSURANCE REQUIREMENTS

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 objective for the TOE. The chosen assurance level is consistent with the claimed threat environment.

Table 6: Assurance Requirements in EAL2

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

8 TOE SUMMARY SPECIFICATION

8.1 OVERVIEW

This chapter provides the TOE summary specification, a high-level definition of the security functions of the TOE and a summary of how those Security Functions meet the SFR's.

8.2 SECURITY FUNCTIONS

Table 7: Mappings of TOE Security Functions and SFRs

	ITSF.I&AUT	TSF.AT&L	ITSF.RETRY_FAIL	ITSF.TIMEOUT	ITSF.ENCRY_DAT	ITSF.SEC_DATA	ITSF.SIGN_MOB
FIA_ATD.1	X						
FIA_AFL.1			X				
FIA_UID.2	X		X				
FIA_UAU.2	X						
FAU_GEN.1		X					
FAU_GEN.2		X					
FPT_STM.1		X					
FAU_SAR.1		X					
FAU_SAR.2		X					
FAU_SAR.3		X					
FAU_STG.1		X					
FTA_SSL.3				X			
FCS_CKM.1					X		
FCS_CKM.4					X		
FCS_COP.1(1)(AES)					X		
FPT_ITT.1						X	
FCS_COP.1(2)(VeriSign)							X

8.2.1 TOE user and group access control

The TOE uses user names and their corresponding passwords for authentication, allowing use of the TOE for authorized users only.

The TOE is designed so that each user, or group of users, can be assigned security attributes, such as specific access rights and privileges, in the operation of the TOE. This covers FIA_ATD.1.

In order to use the TOE functions for which he or she is authorized, based on his or her security attributes, a user must be logged in into the TOE with the correct user name (FIA_UID.2) and corresponding password (FIA_UAU.2).

8.2.2 Three times authentication failure

To prevent brute-force guessing of passwords, the TOE blocks access by disabling an existing user account after a number of unsuccessful authentication attempts. This happens when a user knows the correct user name, but fails to provide the correct password within three tries. This covers FIA_AFL.1.

8.2.3 Encrypted communication channel between TOE Gateway Server and enforcement tools

The TOE implements AES encryption on the data being transferred between the TOE Gateway Server and the NexCode Mobile Application or the NexCode Desktop Application. This is done to prevent unintentional disclosure, and to defeat attempts at interception of and unauthorized access to confidential information flowing between the above components of the TOE. This covers FCS_COP.1(1)(AES).

The TOE includes a random number generator and a key generation function for generating the 128-, 192- or 256-bit AES key, used in the encryption algorithm. This covers FCS_CKM.1.

The TOE administrator also has access to a function of the TOE for erasure of those keys using a proprietary method. This covers FCS_CKM.4.

8.2.4 Trusted TOE mobile application

The TOE implements signing and verification of the NexCode Mobile Application installed on the mobile client.

A signing certificate used on an application serves to protect the integrity of that application by applying a digital signature that is independently verified by VeriSign (FCS_COP.1(2)(VeriSign). A digital signature that does not match warns users that the application has been tampered with or modified, and helps protect them from hackers or malicious code.

8.2.5 Audit trail and logging

The TOE is designed to recognize specific events within its operation and log them. These events include user log-ins and log-outs, a user accessing the NexCode Control Centre Web application, the NexCode Mobile Application, or the NexCode Desktop Application, as well as changes made to the TOE system. This covers FAU_GEN.1.

The information for events logged by the TOE include the user name (FAU_GEN.2) of the account associated with the event, the time and date (FPT_STM.1) of its occurrence, and the nature of the event (e.g., log-in, changes to settings, etc.).

For auditing purposes, logs generated by the TOE may be viewed in human-readable format using a reporting function of the TOE via the Web client (FAU_SAR.1). This ability is allowed only to TOE users who have been authorized to read audit logs on the TOE system (FAU_SAR.2). Such users (i.e., auditors) may choose to view only a specific section of a log or only a specific category of information, sorting and filtering data as necessary (FAU_SAR.3).

The log information used for reporting and audit trails is stored within a database in the TOE, as briefly described in Section 2.3.1.2. The ability to directly access, modify, and/or delete this data within the database is allowed only to TOE users authorized to exercise said abilities, as per Section 8.2.1. This covers FAU_STG.1.

8.2.6 Secure FTP on transferring TOE inventory files

The TOE implements usage of Secure FTP (SFTP) to transport generated inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server. This defeats attempts at unauthorized access and preserves the integrity of the inventory files as they are moved from one TOE server to another. This covers FPT_ITT.1.

8.2.7 Login session idle time-out

The TOE implements a configurable session time-out upon the Web application of the NexCode Control Centre System. By default, 15 minutes without user input causes the TOE to log out the current user, requiring him or her to log in again if use of the TOE is desired. This helps prevent an unauthorized user from using the TOE when the user who is currently logged in leaves the TOE interface unattended. This covers FTA_SSL.3.

9 RATIONALE

9.1 CONFORMANCE CLAIMS RATIONALE

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

9.2 SECURITY OBJECTIVES RATIONALE

9.2.1 Security Objectives for the TOE

Table 8: TOE Security Objectives map to Threats and Organizational Policies

Threat	**How threat is met**
T.ILLEGAL_ACCESS	T.ILLEGAL_ACCESS -> O.AUDIT_LOG, O.TIMEOUT The threat of an authorized TOE user with administrator privileges destroying or disclosing any data or perform operations that are not authorized for each user role is dealt with by implementing: * O.AUDIT_LOG The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to track user activities within the system. When logs are reliable, and unauthorized use is detected correctly and in time, and those users who performed unauthorized actions are given disciplinary action, it serves as a deterrent against unauthorized use. The possibility of being caught serves to diminish the urge to use the system in an unauthorized manner, and therefore reduces the chance of the above threat happening. * O.TIMEOUT The TOE must ensure that the user's access to the system is timed out after a period of idle time. This has the effect of diminishing the chance of the threat happening.
T.BYPASS	T.BYPASS -> O.I&A, O.LOGIN_FAIL The threat that an unauthorized TOE user may successfully violate the authenticity of rules by succeeding in bypassing the authentication is dealt with by applying: * O.I&A The TOE must provide login and user identification and authentication by allowing only authorized username and authenticated password to gain access to the system having access rights controlled by either an

	individual user or a user group. This has the effect of greatly diminishing the chance of the above threat happening. The threat cannot be removed entirely because of the possibility, however small, that a username and its password can be guessed or otherwise illegally acquired. * O.LOGIN_FAIL The TOE must prevent or block users from login into the system after three attempts with incorrect passwords. This has the effect of greatly diminishing the chance of the threat happening.
T.DATA_INTERCEPT	T.DATA_INTERCEPT -> O.ENCRYPT_DATA, O.SECURE_DATA Experienced hackers may maliciously listen and tamper with: o The data along the communication channel between the TOE Gateway Server and the mobile client or the desktop client; o The transferring of TOE inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server; o The HTTP request for any TOE Web client access to NexCode Control Centre System. These activities can be dealt with by executing the following: * O.ENCRYPT_DATA The TOE must ensure that the TOE data along communication channel between the TOE Gateway Server and the mobile client or the desktop client is encrypted using AES encryption. This has the effect of greatly diminishing the chance of the above threat happening. The threat cannot be removed entirely because of the possibility, however small, that malicious individuals with access to vast technical resources may be able to decrypt the communications. * O.SECURE_DATA The TOE must ensure that the TOE inventory files (NexCode 2D barcode images) transferred from the TOE Inventory Server to the TOE Load Server is via the Secure FTP (SFTP). This has the effect of greatly diminishing the chance of the above threat happening.
T.UNTRUSTED_APP	T.UNTRUSTED_APP -> O.SIGN_MOB TOE user that accesses the TOE mobile application may be using an unsigned product. This can be mitigated with the following objective: * O.SIGN_MOB The TOE must ensure that the TOE mobile application is signed and verified.
P.ADMIN_IDENTIFY	P.ADMIN_IDENTIFY -> O.I&A

	Authorized System Administrator and the Auditor who use the TOE are subject to the TOE identification to keep a record of TOE access logs. * O.I&A The TOE must provide login and user identification and authentication by allowing only authorized username and authenticated password to gain access to the system having access rights controlled by either an individual user or a user group.
P.AUDIT_LOG	P.AUDIT_LOG -> O.AUDIT_LOG The ability to access the TOE audit logs is to be restricted to the Auditor only in order to track unauthorized operations on the TOE assets to be protected. * O.AUDIT_LOG The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to track user activities within the system. This has the effect of supporting the policy of segregation of duties between auditors and system administrators. It must be enforced because of two major benefits: 1. deliberate misuse becomes more difficult because it requires conspiracy between two or more persons, and 2. it becomes much more likely that accidental errors will be positively identified. System administrators who are restricted to operating their assigned hardware and software are discouraged from unauthorized use by the knowledge that some other authorized person will be reporting their actions. Auditors who are restricted to observing and reporting are prevented from exploiting their knowledge of the system to perform unauthorized use.

9.2.2 Security Objectives for the Operational Environment

Table 9: Mapping of Security Objectives for the Operational Environment to Assumptions

Assumption	How assumption traced back to objective for operational environment
A.PHY_ACC	A.PHY_ACC –> OE.PHYSEC This objective for the operating environment ensures that the assumption is upheld that the TOE is physically secured and located within a secure controlled access facility, which will prevent unauthorized physical access or modification. The TOE security objective presented to address this assumption is: OE.PHYSEC

A.TIME	A.TIME --> OE.TIME The objective for the operating environment ensures that that the assumption is upheld that the TOE is provided a reliable time source for the TOE to provide an accurate timestamp for all audit records. The TOE security objective presented to address the assumption is: OE.TIME

9.3 SECURITY REQUIREMENTS RATIONALE

9.3.1 Tracing of SFR to Security Objectives

The functional and assurance requirements presented in this ST are mutually supportive and their combinations meet the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. *Table 10* illustrates the mapping between the security requirements and the security objectives. *Table 11* demonstrates the relationship between the assumptions, threats, policies and TOE security objectives. Together these tables demonstrate the completeness and sufficiency of the requirements.

Table 10: Mappings of SFR and TOE Security Objectives

	O.I&A	O.AUDIT_LOG	O.LOGIN_FAIL	O.TIMEOUT	O.ENCRYPT_DATA	O.SECURE_DATA	O.SIGN_MOB
FIA_ATD.1	X						
FIA_AFL.1			X				
FIA_UID.2	X		X				
FIA_UAU.2	X						
FAU_GEN.1		X					
FAU_GEN.2		X					
FPT_STM.1		X					
FAU_SAR.1		X					
FAU_SAR.2		X					
FAU_SAR.3		X					
FAU_STG.1		X					
FTA_SSL.3				X			
FCS_CKM.1					X		
FCS_CKM.4					X		
FCS_COP.1(1)(AES)					X		
FPT_ITT.1						X	
FCS_COP.1(2)(VeriSign)							X

FIA_ATD.1 User attribute definition: This component specifies the security attributes that should be maintained at the level of the user. This means that the security attributes listed are assigned to and can be changed at the level of the user. In other words, changing a security attribute in this list associated with a user should have no impact on the security attributes of any other user. This component traces back to and aids in meeting the following objective: **O.I&A.**

FIA_AFL.1 Authentication failure handling: This component requires that the TSF be able to terminate the session establishment process after three consecutive unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs. This component traces back to and aids in meeting the following objective: **O.LOGIN_FAIL**.

FIA_UID.2 User identification before any action: This component poses requirements for the user to be identified before any TSF-mediated actions can be performed in behalf of that user. This component traces back to and aids in meeting the following objective: **O.I&A** & **O.LOGIN_FAIL**.

FIA_UAU.2 User authentication before any action: This component requires that a user is authenticated before any other TSF- mediated action can take place on behalf of that user. This component traces back to and aids in meeting the following objective: **O.I&A**.

FAU_GEN.1 Audit data generation: This component defines requirements to identify the auditable events for which audit records should be generated, and the information to be provided in the audit records. This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FAU_GEN.2 User identity association: This component addresses the requirement of accountability of auditable events at the level of individual user identity. This component should be used in addition to FAU_GEN.1 Audit data generation. This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FPT_STM.1 Reliable time stamps: Some possible uses of this component include providing reliable time stamps for the purposes of audit as well as for security attribute expiration. This component traces back to and aids in meeting the following objective: **OE.TIME**.

FAU_SAR.1 Audit review: This component will provide authorized users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion. This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FAU_SAR.2 Restricted audit review: This component specifies that any users not identified in FAU_SAR.1 Audit review will not be able to read the audit records. This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FAU_SAR.3 Selectable audit review: This component is used to specify that it should be possible to perform selection of the audit data to be reviewed. If based on multiple criteria, those criteria should be related and the tools should provide the ability to manipulate audit data (e.g. sort, filter). This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FAU_STG.1 Protected audit trail storage: This component specifies that requirements are placed on the audit trail. It will be protected from unauthorized deletion and/or modification. This component traces back to and aids in meeting the following objective: **O.AUDIT_LOG**.

FTA_SSL.3 TSF-initiated termination: This component provides requirements for the TSF to terminate the session after a specified period of user inactivity. This component traces back to and aids in meeting the following objective: **O.TIMEOUT**.

FCS_CKM.1 Cryptographic key generation: This component requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes which can be based on an assigned standard. This component traces back to and aids in meeting the following objective: **O.ENCRYPT_DATA.**

FCS_CKM.4 Cryptographic key destruction: This component requires cryptographic keys to be destroyed in accordance with a specified destruction method which can be based on an assigned standard. This component traces back to and aids in meeting the following objective: **O.ENCRYPT_DATA**.

FCS_COP.1(1) Cryptographic operation (AES): This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation(s) which can be based on an assigned standard. This component traces back to and aids in meeting the following objective: **O.ENCRYPT_DATA.**

FPT_ITT.1 Basic internal TSF data transfer protection: This component requires that TSF data be protected when transmitted between separate parts of the TOE. This component traces back to and aids in meeting the following objective: **O.SECURE_DATA.**

FCS_COP.1(2) Cryptographic operation (VeriSign): This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation(s) which can be based on an assigned standard. This component traces back to and aids in meeting the following objective: **O.SIGN_MOB**.

9.3.2 Tracing of Security Objectives to Security Problem Definition

The relation between security objectives and the security problem definition (threats, organizational security policies and assumptions) is shown in *Table 11*.

Table 11: Mappings of TOE Security Objectives and Security Problem Definition

	T.ILLEGAL_ACCESS	T.BYPASS	T.DATA_INTERCEPT	T.UNTRUSTED_APP	P.ADMIN_IDENTIFY	P.AUDIT_LOG	A.PHY_ACC	A.TIME
O.I&A		X			X			
O.AUDIT_LOG	X					X		
O.LOGIN_FAIL		X						
O.TIMEOUT	X							
O.ENCRYPT_DATA			X					
O.SECURE_DATA			X					
O.SIGN_MOB				X				
OE.PHYSEC							X	
OE.TIME								X

9.3.3 SFR Dependency Rationale

Table 12: SFR dependency rationale

SFR	Dependency	Justification
FIA_ATD.1	None	No dependencies to satisfy.
FIA_AFL.1	FIA_UAU.1	Satisfied with FIA_UAU.2.
FIA_UID.2	None	No dependencies to satisfy.
FIA_UAU.2	FIA_UID.1	Satisfied with FIA_UID.2.
FAU_GEN.1	FPT_STM.1	Satisfied with FPT_STM.1.
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Satisfied with FAU_GEN.1 and FIA_UID.2.
FPT_STM.1	None	No dependencies to satisfy.
FAU_SAR.1	FAU_GEN.1	Satisfied with FAU_GEN.1.
FAU_SAR.2	FAU_SAR.1	Satisfied with FAU_SAR.1.
FAU_SAR.3	FAU_SAR.1	Satisfied with FAU_SAR.1.
FAU_STG.1	FAU_GEN.1	Satisfied with FAU_GEN.1.
FTA_SSL.3	None	No dependencies to satisfy.
FCS_COP.1(1)(AES)	FCS_CKM.1, FCS_CKM.4	Satisfied with FCS_CKM.1 and FCS_CKM.4.
FPT_ITT.1	None	No dependencies to satisfy.
FCS_COP.1(2) (VeriSign)	FCS_CKM.1, FCS_CKM.4	None satisfied, because the TSF only verifies the integrity of the Mobile Application with Verisign. The TSF has no need to generate (nor destroy) cryptographic keys for this process. Therefore, FCS_CKM.1 and FCS_CKM.4 are not applicable.

9.3.4 SAR Justification

The security assurance requirements that are selected for the TOE are from the CC EAL2 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.