SECURITY TARGET:

SQ-PHOENIX DIGITAL ENCRYPTOR

VERSION 2.7

Prepared by and for:

CES Communications Ltd

Version 1.3

March 2004

TABLE OF CONTENTS

INDEX OF TABLES

1 Security Target Introduction

A Security Target (ST) provides the basis for an evaluation of an information technology (IT) security product or system, known within the ST as the Target of Evaluation (TOE), in accordance with the requirements of the Common Criteria (CC).

The ST defines:

a) a security problem and a description of the TOE environment, allowing identification of threats which the TOE is intended to counter;
b) security objectives giving information about how, and to what extent, the security needs are to be met by the TOE;
c) a set of security functional requirements reporting the role of the TOE and the role of the TOE's environment in meeting the security objectives;
d) a set of assurance requirements reporting the degree of confidence which may be expected in the TOE Security Functions (TSFs) in respect of meeting the objectives; and
e) a rationale demonstrating that the stated requirements are sufficient to address the security problem, and that the TOE meets these requirements.

1.1 ST and TOE Identification

This section provides the information necessary to identify the version of ST and TOE under evaluation. This ST targets an Evaluation Assurance Level (EAL) 2 level of assurance.

ST Title:	Security Target: SQ-Phoenix Digital Encryptor Version 2.7. Version 1.3, March 2004
TOE Identification:	SignalGuard SQ-Phoenix Digital Encryptor Version 2.7
ST Evaluation:	Australasian Information Security Evaluation Programme, Tenix AISEF
Authors:	Sarah Macann, Malcolm Shore
Keywords:	Security target, encryption, voice encryptor, fax encryptor
CC Version:	Version 2.1, 1999

1.2 ST Overview

The SignalGuard SQ-Phoenix Digital Encryptor (SQ-Phoenix) is an in-line encryptor for voice and fax communications over analog transmission networks. As such, it is a device primarily designed to protect the confidentiality of sensitive information during transmission. The SQ-Phoenix takes data from the operator's communications equipment, digitises it if necessary, and encrypts it for transmission in digital form across the communications network. Digital transmission across the analog network is accomplished using the V32.bis modem protocol and commercial communications components.

The SQ-Phoenix is administered and managed by authenticated users. The SQ-Phoenix can be operated by any individual with physical access to the unit and the operator chooses whether to invoke the SQ-Phoenix's security functions. In the evaluated configuration, encryption is performed using the AES128 digital encryption algorithm and 128-bit keys. The evaluated configuration comprises a subset of the SQ-Phoenix's total functionality.

The SQ-Phoenix provides single-session operation and cannot be used for multiple concurrent secure communication sessions even by the same operator.

The SQ-Phoenix has been designed for deployment in a wide variety of telecommunications situations and has selectable settings to ensure smooth operation in the local environment.

The TOE comprises a specific subset of the SQ-Phoenix's complete functionality as described within this document.

1.3 CC Conformance

This ST conforms in structure and content with the requirements specified Parts 2 and 3 of the CC, Version 2.1.

1.4 Definitions

The following phrases are used with specific meaning in this document:

Administrator – an administrative role authenticated by entering the correct Administrator password for the SQ-Phoenix. The Administrator is responsible for ensuring that the SQ-Phoenix operates correctly in its communications environment. The Administrator has no responsibility for cryptographic configuration or secure operation. Assumption of the Administrator role allows communications related settings (but not cryptographic settings) to be viewed and/or changed (for a full description of each item, please refer to the Administrator Guidance). Configuration items available to the Administrator are as follows:

CONFIGURATION ITEM	VIEW	CHANGE
Administrator password		X
Unit identity	X	X
Fax authentication identifier	X	X
Select Communications Default	X	X
Select Modem Speed	X	X
Set Signal Level	X	X
Set Volume Level	X	X
Select Impedance	X	X

An individual with Administrator privileges may at times also assume the role of Operator.

Crypto-Custodian – Crypto-Custodian is a role authenticated by entering the correct Crypto-Custodian password for the SQ-Phoenix. The Crypto-Custodian is responsible for ensuring that the SQ-Phoenix is correctly configured for secure operation. Access to configuration items affecting security settings is restricted to the Crypto-Custodian.

Assumption of the Crypto-Custodian role automatically confers access to all items available to an Administrator except the ability to change the Administrator password. In addition to Administrator functions, the Crypto-Custodian has access to view and/or change the following configuration settings.

CONFIGURATION ITEM	VIEW	CHANGE
Crypto-Custodian password		X
Select Cryptographic Mode	X	X
Select default key number	X	X
Select algorithm	X	X
Select cipher chaining mode	X	X
Execute keyfill	X	X
Configure Customer Code		X
Configure Group Mode KEKs		X

Operator – an individual who is using the SQ-Phoenix in order to perform secure communications. The operator is implicitly authorised by virtue of access to the equipment; there is no explicit authentication by the SQ-Phoenix. The operator can perform the following actions:

– activate the SQ-Phoenix's secure communication function;

– override the SQ-Phoenix's default configuration to select or bypass security for a fax transmission;

– override the SQ-Phoenix's default configuration to select a specific key for a secure communication; and

– alter the "update" cycle setting.

The role of operator cannot be assumed concurrently with an explicitly authenticated role.

Sensitive communication – a transmission of sensitive information over a public transmission network.

Sensitive information – the information content of a voice or fax communication which the user organisation wishes to keep confidential.

Sensitive cryptographic material – secret key information generated by the user organisation for use in the SQ-Phoenix for key exchange.

User– any individual interacting with the SQ-Phoenix without specification of role. The user may be acting as an operator, Administrator or Crypto-Custodian.

User organisation – the organisation which has deployed the SQ-Phoenix to protect its sensitive information, and the individuals with administrative responsibility for the SQ-Phoenix network within that organisation.

2 TOE Description

This section provides background information to the TOE and provides context for the evaluation by identifying the product, its intended role in the security environment, and the evaluated configuration.

2.1 Overview of the TOE

The TOE comprises a specific configuration and functionality set of the SQ-Phoenix Digital Encryptor unit. Units must be set to this configuration prior to deployment. Operating functions available from the SQ-Phoenix but which are not included within the TOE are outlined in Section 2.5, Non-Evaluated Features. Ancillary support equipment is not included within the TOE.

2.1.1 TOE Security Functions

The SQ-Phoenix is an in-line encryptor for voice and fax communications (CCITT Group III) over analog networks.

The SQ-Phoenix provides protection of sensitive communications by encrypting the sensitive information before it is transmitted across the vulnerable transmission path. This protects against loss of **confidentiality**.

The SQ-Phoenix protects the confidentiality of sensitive cryptographic material by storing it in secure memory within the microcontroller, protected by hardware security locks. Zeroise mechanisms (emergency erase and anti-tamper) erase the keys in the event that physical violation is detected. The SQ-Phoenix does not support export of cryptographic variables to any user.

The SQ-Phoenix protects against compromise of both sensitive information in the clear and of sensitive cryptographic material by ensuring that this information is shielded from the line and may not be passed into the insecure environment by electromagnetic radiation.

The SQ-Phoenix also protects against loss of **integrity** because information cannot be modified, substituted or inserted into the encrypted data stream.

The SQ-Phoenix confirms the authorisation of the remote operator for access to sensitive information, by requiring that both participants in a secure session have access to equipment programmed with the same cryptographic keys. If the cryptographic configuration of the remote equipment is not identical to the originating SQ-Phoenix, the originator declines the communication. This provides assurance that that operator is authorised to communicate securely with the local party.

The SQ-Phoenix also provides a recipient **authentication** function for secure fax transmissions, preventing accidental transmission of a document containing sensitive information to other than the intended recipient.

2.1.1.1 Encryption Functions

The SQ-Phoenix performs encryption using the AES128 algorithm and externally generated 128 bit keys.

2.1.1.2 Cryptographic Support Functions

The SQ-Phoenix accepts an externally generated key table of 128-bit key exchange keys (KEKs) which has been encrypted with a 128-bit transfer key and which is loaded into the SQ-Phoenix for immediate activation and use. Key expiry dates are set in procedure and are not inherently associated with the key table. The SQ-Phoenix supports multiple cryptographic keys to allow compartmentalisation.

The SQ-Phoenix generates 128-bit one-time traffic encryption keys (TEKs) using an internal hardware random number generator, and may generate 128-bit KEK "updates", using a pseudo-random process seeded by the KEKs generated by the user organisation and stored in the device.

2.1.1.3 Authentication Functions

The SQ-Phoenix authenticates its users before allowing access to modify configuration settings. The SQ-Phoenix supports the role of operator, and the administrative roles of Administrator and Crypto-Custodian. Authentication to an administrative role is by password. Authentication to the role of operator is implicit from access to the SQ-Phoenix in its operating location.

The SQ-Phoenix can be requested to authenticate the recipient in a secure fax transmission to prevent accidental transmission of sensitive information to an authorised recipient other than the intended recipient.

2.1.1.4 Physical Security Countermeasures

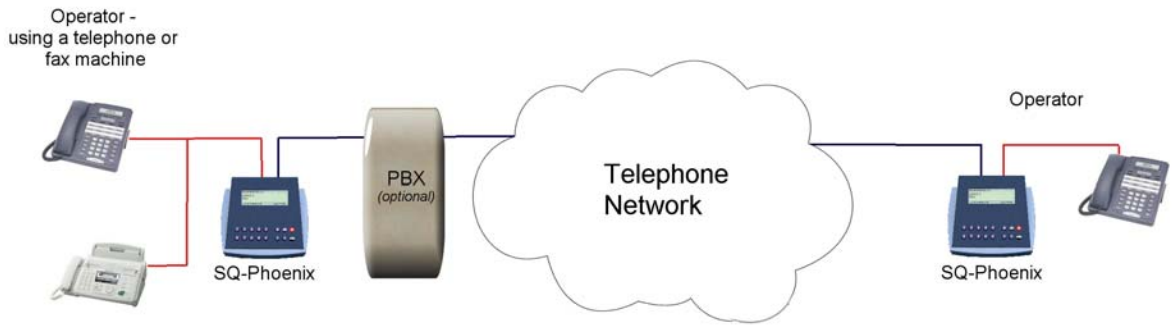
Physical security countermeasures are implemented to protect the SQ-Phoenix against compromise by physical violation. The SQ-Phoenix provides a zeroise function which may be activated in two ways. The operator can zeroise stored sensitive cryptographic material deliberately via a switch on the rear of the unit, in the event that the unit will be unprotected in transit or if the unit's physical security is in immediate danger of compromise; or the SQ-Phoenix will automatically zeroise its sensitive cryptographic material if the unit is opened.

2.1.2 Operation

The SQ-Phoenix takes data from the operator's communications equipment, digitises it (where necessary) and encrypts it before transmitting it across the communications network. Digital transmission across the analog network is accomplished using the V32.bis modem protocol and commercial communications components.

The SQ-Phoenix has been designed for maximum flexibility in operation and maximum user-friendliness. It can be configured to provide a variety of levels of security, according to the requirements and technical support capabilities of the user organisation. When its security functions are not required, the SQ-Phoenix will not interfere with normal communications.

The SQ-Phoenix is installed into its operating communications network as represented below:



A typical use of the SQ-Phoenix for voice communication follows the process below:

i) The operator uses the telephone to initiate a connection across the network.

ii) When the connection is established, the operator activates the SQ-Phoenix to request a secure session.

iii) The SQ-Phoenix confirms the presence of another SQ-Phoenix unit at the remote end of the communication and attempts to establish a modem connection.

iv) If the modem connection is successfully established, the SQ-Phoenix requests a secure session.

v) If the two units are in a compatible configuration, the request is accepted and the session enters secure state.

vi) The communication continues until the operator terminates the connection, or both operators terminate secure state.

Error messages are returned if there is no SQ-Phoenix at the remote end, a modem connection cannot be established, or the cryptographic configuration of the two units is not compatible.

A typical use of the SQ-Phoenix for fax communication follows the process below:

i) The operator uses the fax machine to initiate a connection across the network.

ii) The SQ-Phoenix automatically activates and attempts to confirms the presence of another SQ-Phoenix at the remote end of the communication.

iii) If remote equipment is present, the SQ-Phoenix attempts to establish a modem connection.

iv) Each SQ-Phoenix emulates a fax machine to communicate with its local fax machine.

v) If the modem connection is successfully established, the SQ-Phoenix attempts to authenticate the unit as the intended recipient (if authentication is requested by the sender).

vi) If the recipient is authenticated, the SQ-Phoenix requests a secure session.

vii) If the two units are in a compatible configuration, the request is accepted and the session enters secure state.

viii) The data from the sending fax machine is accepted by the local SQ-Phoenix and is encrypted and passed across the modem connection, then decrypted by the remote unit and relayed to its local fax machine for processing.

ix) The connection terminates automatically at the conclusion of the document.

Error messages are returned if there is no SQ-Phoenix at the remote end, a modem connection cannot be established, the remote unit's fax authentication identifier does not match that entered by the operator sending the document, or the cryptographic configuration of the two units is not compatible.

2.2 Operating Environment

The SQ-Phoenix is an end-user device which has been designed to be cryptographically configured by an authorised Crypto-Custodian, but which may be operated by any operator with physical access to the equipment. Accordingly, individuals with access to the SQ-Phoenix must be suitably vetted and trained as authorised operators.

The requirement for operation over analog communication networks limits the application context to systems such as the public switched telephone network (PSTN) or full bandwidth analog satellite circuits. However, connection to these networks may be mediated by network equipment such as a private exchange (PABX). The SQ-Phoenix's behaviour does not depend on the behaviour or nature of the communications network, and the communications network does not constitute a part of the TOE. The presence or absence of intervening equipment is irrelevant to the SQ-Phoenix.

The SQ-Phoenix interacts with its environment via a local connection to communications equipment (a telephone or fax machine) and a network connection to the PSTN (optionally via a PABX), or satellite terminal equipment. The SQ-Phoenix 's behaviour does not depend on the behaviour or nature of the communications equipment, and the communications equipment does not constitute a part of the TOE.

The SQ-Phoenix also interacts via a DB9 serial port on the rear of the unit, which allows a Crypto-Custodian to load an encrypted table of externally generated keys into the SQ-Phoenix in a specified format.

2.3 Scope and Boundary

2.3.1 Physical Scope

The SQ-Phoenix is an electronic device enclosed in an ABS plastic case. Operator input is provided via a 16 button keypad and feedback is via a graphical LCD. The equipment comprises three separate printed circuit assemblies, one providing general unit functions and central control, one dedicated to cryptographic operation, and one performing input/output mediation for the user interface. An internal self-charging battery provides a back-up power source in case of mains power loss.

The unit is connected to the communications network by telephone cables to standard RJ-11 sockets on the rear of the device. One socket is required for connection to the network and one to the local telephone equipment. When the device's secure functions are not required, a relay enables the unit to operate in clear bypass mode for minimum disruption to normal communications practice.

2.3.2 Logical Scope and Boundary

With the exception of the circuitry dedicated to cryptographic operation, the SQ-Phoenix is constructed as a generic communications device and all functions are controlled via software modules run on the

unit's host processor, an Atmel AVR. Separate software modules perform operations for configuration menu access, user interface, and cryptographic session control.

2.4 Evaluated Configuration

In the TOE configuration, the SQ-Phoenix is configured before deployment to use the Advanced Encryption Standard 128 bit (AES128) algorithm in Cipher Feedback (CFB) mode, with 128-bit keys. Key exchange keys are generated by the customer externally, and are outside the scope of the Evaluation. Traffic exchange keys are generated within the SQ-Phoenix. The mathematical qualities of the AES128 algorithm are outside the scope of the Evaluation.

The evaluated configuration uses a key management configuration termed "Net Mode". In this configuration, the SQ-Phoenix is electronically loaded with externally-generated 128-bit keys for use in key exchange. One-time 128-bit keys for traffic exchange are generated internally at the start of each secure session.

The evaluated configuration includes both voice and fax operation.

2.5 Non-Evaluated Features

The SQ-Phoenix supports alternative configurations and functions outside the scope already outlined. These comprise:

2.5.1 Configurations

All key management configurations other than Net Mode
Encryption using cryptographic algorithms other than AES128
Cipher chaining in electronic codebook mode
Operation without dedicated cryptographic circuitry

2.5.2 Functions

Secure file transfers over the secure voice link

Communications preferences (unit identity, communications default, modem speed, signal and volume level, impedance) do not affect the conduct of secure operation and are not considered within this ST.

2.6 TOE Security Services

The TOE provides the following security features:

Name	Description
System administration	Maintain system configuration information
Authentication and verification	Authenticate users and validate user actions
System self-testing	Confirm system integrity at start-up
System status feedback	Confirm system status during operation
Manage TEKs	Generate traffic exchange keys for use
Manage KEKs	Securely store traffic exchange keys for use
Manage KEK updates	Derive key exchange key updates for use
Communications session management	Establish and maintain the communications channel
Secure session management	Establish security across the communications channel
Encryption/decryption	Encrypt and decrypt data for voice and fax communications
Tamper response	Detect and respond to violations of physical integrity

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section details assumptions about security aspects of the TOE's environment and operation; the nature and danger posed by threats which the TOE (or its operating environment) must protect against; and organisation security policies with which the TOE must comply in addressing security needs.

3.1 Assumptions

The following assumptions are made relating to the operation of the TOE:

Table 1. Assumptions

Name	Description
A.ADMIN_TRUSTED	Administrators and Crypto-Custodians are non-hostile and follow all administrator guidance and abide by all organisational security policies.
A.ASSET	The asset to be protected by the TOE is the information content of a voice or fax communication. The user organisation values the protected asset.
A.BYPASS	An operator must choose whether or not to invoke the security functions available from the TOE.
A.COMPARTMENTALISE	Operators may not be equally privileged for have access to all sensitive information. The TOE will be configured to reflect its operator's access privileges.
A.EMR	The TOE incorporates measures to ensure that electromagnetic radiation does not allow cryptographic variables or sensitive information to be transmitted without protection into the insecure environment.
A.KEYMAN_EXT	128-bit KEKs are generated externally of and completely separately from the TOE. This sensitive cryptographic material is generated to a high standard in a controlled environment, and is protected by safeguards in distribution and handling.
A.LOCATE	The TOE will be operated in a controlled environment which has been secured in accordance with the guidance in the SQ-Phoenix Installation and Start-Up Guide. All individuals with authorised physical access to the installed location are assumed to be authorised to operate the TOE.
A.USER_TRUSTED	Users comply with TOE policies of use and cooperate to maintain TOE security. Users are trusted to the extent required to correctly carry out their authorised role(s).

3.2 Threats

Threats may be addressed by the TOE, or by its intended environment (including physical, administrative or procedural safeguards).

The TOE addresses the following threats:

Table 2. Threats addressed by the TOE

Name	Description
T.ABUSE	An operator may attempt to breach the TSP in order to gain unauthorised access to sensitive information, including sensitive cryptographic material.
T.CAPTURE_CRYPTO	An attacker is likely to attempt to intercept cryptographic key material or cryptographic session information which might assist recovery of intercepted encrypted sensitive information.
T.CAPTURE_INFO	An attacker is likely to attempt to intercept and capture sensitive information while being transmitted across the communications network.
T.CRACK	An attacker is likely to attempt to perform cryptanalysis on transmitted information to gain access to sensitive cryptographic material or sensitive information.
T.EXTRACT	A user or an attacker may attempt to extract sensitive cryptographic material from the TOE.
T.HARDWARE_FAIL	A hardware error within the TOE may prevent the TOE from operating in the intended manner, compromising the TOE's protection of sensitive information during transmission.
T.WRONG_FAX	An operator may inadvertently attempt to send a document containing sensitive information to an authorised recipient who is not the intended recipient.

The following threats are addressed by the TOE's operating environment:

Table 3. Threats addressed by the operating environment

Name	Description
TE.ADMIN_ERROR	An Administrator or Crypto-Custodian may accidentally configure the TOE in a manner which causes it to not behave in the manner for which it was designed, thereby reducing the protection provided by its security functions.
TE.INSTALL	A user may install the TOE in a manner which causes it to not behave in the manner for which it was designed, thereby reducing the protection provided by its security functions.
TE.UNAUTHORISED	A user or attacker may attempt to gain unauthorised access to operate, subvert or analyse the TOE.

3.2.1 Characterisation of threats and threat agents

Unauthorised use

The threat agent is an operator who deliberately attempts to use the TOE to gain access to sensitive information or sensitive cryptographic material for which the user is not authorised. Inadvertent and accidental use of the TOE in a manner whereby an operator appears to be attempting access to unauthorised information is not included within this threat.

i) **Expertise – Low**. Operators are end users and are typically not technically proficient. Although the operator will be familiar with the operation of the TOE, he will not be well-versed in its configuration and control. He will not have access to network information which might assist in compromising the equipment.

ii) **Resources – Low**. The operator would not have access to the information required to reconfigure the TOE to simulate access authorisation (Crypto-Custodian password information). The operator would not have unlimited time to devote to the attack as the probability of detection would be extremely high.

iii) **Motivation – Low**. Success in gaining access to the TOE's information channel does not mean the operator would automatically gain access to the desired information. Access to sensitive information would require the other party to the communication to be deceived or persuaded into sharing the protected information. Any benefit to the operator from the information would be offset by the likely repercussions of being detected – termination of employment and possibly legal action.

iv) **Other factors**. The TOE does not support export of sensitive cryptographic material to any user. The likelihood of successfully gaining access to sensitive cryptographic material is negligible.

External attack

The threat agent is any external entity not authorised to access the protected asset and who wishes to gain unauthorised access. The threat agent ("attacker") may be an individual or a group of individuals.

i) **Expertise – High**. An attacker is likely to be proficient in the operation and behaviour of the TOE. The attacker is likely to have substantial technical expertise and may have previous experience with the TOE as an operator and/or an Administrator or Crypto-Custodian.

ii) **Resources – High**. The attacker would not have direct access to the system, but would have passive access for observation of sensitive communications by interception of data in transit. The attacker would have access to substantial, but not unlimited, resources for interception and processing of communications data. The attacker would have unlimited time to gather data as the passive method would mean that the attack and even the existence of the attacker would likely go undetected.

iii) **Motivation – High**. The attacker would be highly motivated to gain access to the protected asset.

3.3 Organisational Security Policies

The following organisational security policies are relevant to the operation of the TOE:

Table 4. Organisational Security Policies

Name	Description
P.CONFIDENTIALITY	Adequate equipment, personnel, training and support resources will be commissioned in order that the confidentiality of sensitive information can be protected when transmitted over insecure networks.
P.CRYPTO	Technical and physical assurance procedures will be defined and rigorously enforced for generation, distribution, change and handling of all cryptographically relevant material.

P.PASSWORDS	Procedures will be defined and enforced relating to the management of passwords, including requirements for password length, frequency of change, handling and record keeping, and quality (non-predictability).

4 Security Objectives

The security objectives detail the intended response to the identified security problem. These objectives indicate, at a high level, how the security problem (defined in Section 3) is to be addressed.

4.1 Security Objectives for the TOE

The security objectives to be satisfied by the TOE are specified in the table below:

Table 5. Security Objectives for the TOE

Name	Description
O.ACCESS_CONTROL	The TOE must prevent operators from deliberately or accidentally altering the TOE's configuration to effect a change to their information access privileges.
O.AUTHENTICATE_RECIPIENT	The TOE must provide a means for the operator to ensure that a document containing sensitive information can only be sent to the intended recipient.
O.BLACK_TRANSFER	The TOE must provide the Crypto-Custodian with a means of loading sensitive cryptographic material in an encrypted format.
O.COMPARTMENTALISE	The TOE must support multiple cryptographically compartmentalised groups for differential access to sensitive information. The TOE must provide the Crypto-Custodian with a means of configuring the TOE to reflect compartmentalisation.
O.CONFIDENTIALITY	The TOE must provide operators with a reliable means of confidentially exchanging sensitive information.
O.REPORT_STATUS_CRYPTO	The TOE must report to its operator and the operator of the remote SQ-Phoenix if the TOE fails to secure its communications session.
O.REPORT_STATUS_SESSION	The TOE must report to its operator its current operating status.
O.REPORT_STATUS_SYSTEM	The TOE must report to its operator any system errors which may affect correct operation.
O.SECRET_KEY_EXCHANGE	The TOE must provide a means to protect the confidentiality and integrity of cryptographic traffic keys when exchanged across an insecure network.
O.SECRET_KEY_STORE	The TOE must provide a means to protect the confidentiality and integrity of sensitive cryptographic material stored within the TOE.
O.STORE_SECURE	The TOE must not allow sensitive cryptographic material to be extracted from the TOE.

4.2 Security Objectives for the Environment

The security objectives to be satisfied by the TOE environment are specified in the table below:

Table 6. Security Objectives for the Environment

Name	Description
OE.EDUCATE	Those responsible for the management of the TOE must ensure that all operators are aware of the TOE's functions and operation, and are given sufficient training to enable them to operate the TOE correctly and securely.
OE.INSTALL	The TOE's Crypto-Custodian must ensure that the TOE is configured and installed in a manner that enables it to perform its communications security functions in accordance with the user organisation's policies for communications security.
OE.LOOK_FIRST	Those responsible for the management of the TOE must ensure that all operators are aware that the TOE can operate in a secure bypass mode, can recognise the TOE's indications of secure and bypass modes, and will check for these indications before operating the TOE to pass sensitive information.
OE.MANAGE_KEYS	Those responsible for the management of the TOE must ensure that technical and procedural measures are in place to ensure that sensitive cryptographic material for use in the TOE is prepared and managed in a manner consistent with the strength of security protection required of the TSF.
OE.MANAGE_PASSWORDS	Those responsible for the management of the TOE must ensure that procedural measures are in place to ensure that passwords are generated and managed in a manner consistent with organisational security policy.
OE.TAMPER_EVIDENT	The TOE's operator must be able to detect whether the TOE has been physically violated.
OE.TRAIN	Those responsible for the management of the TOE must ensure that all users given Administrator or Crypto-Custodian privileges are given training sufficient to enable them to perform their duties securely.
OE.VET	The user organisation must ensure that all users are trustworthy to the extent required to ensure reliable and responsible execution of their highest authorised role.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section contains the security functional requirements (SFRs) for the TOE, derived from the CC Part 2 Security Functional Requirements. The overall Strength of Function claim for the TOE is SOF-basic. The SFRs are summarised in the table below:

Table 7. TOE Security Functional Requirements

No.	Component	Component Name
Class FCS: Cryptographic Support		
1	FCS_CKM.1(1)	Cryptographic key generation (TEKs)
2	FCS_CKM.1(2)	Cryptographic key generation (KEK Updates)
3	FCS_CKM.2	Cryptographic key distribution
4	FCS_CKM.4(1)	Cryptographic key destruction (KEK replacement)
5	FCS_CKM.4(2)	Cryptographic key destruction (KEK zeroise)
6	FCS_CKM.4(3)	Cryptographic key destruction (KEK Updates)
7	FCS_CKM.4(4)	Cryptographic key destruction (TEKs)
8	FCS_COP.1(1)	Cryptographic operation (Data encryption/decryption)
9	FCS_COP.1(2)	Cryptographic operation (Cryptographic support)
Class FDP: User Data Protection		
10	FDP_IFC.1	Subset information flow control
11	FDP_IFF.1	Simple security attributes
12	FDP_UCT.1	Basic data exchange confidentiality
Class FIA: Identification and Authentication		
13	FIA_UAU.1	Timing of authentication
14	FIA_UAU.7	Protected authentication feedback
Class FMT: Security Management		
15	FMT_MOF.1	Management of security functions behaviour
16	FMT_MTD.1(1)	Management of TSF data (Cryptographic configuration)
17	FMT_MTD.1(2)	Management of TSF data (Fax ID)
18	FMT_MTD.1(3)	Management of TSF data (Crypto-Custodian password)
19	FMT_MTD.1(4)	Management of TSF data (Administrator password)
20	FMT_MTD.1(5)	Management of TSF data (KEK selection)
21	FMT_SMR.1	Security roles

22	FMT_SMR.3	Assuming roles
Class FPT: Protection of the TSF		
23	FPT_AMT.1	Abstract machine testing
24	FPT_ITA.1	Inter-TSF availability within a defined availability metric
25	FPT_ITC.1	Inter-TSF confidentiality during transmission
26	FPT_ITI.1	Inter-TSF detection of modification
27	FPT_PHP.3	Resistance to physical attack
Class FTA: TOE Access		
28	FTA_TSE.1	TOE session establishment
Class FTP: Trusted Path/Channels		
29	FTP_ITC.1	Inter-TSF trusted channel

5.1.1 Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic Key Generation (TEKs)

Hierarchical to: No other components

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*non-deterministic source: ring oscillator*] and specified cryptographic key sizes [*128 bits*] that meet the following: [*none*].

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_COP.1 Cryptographic operation
FMT_MSA.2 Secure security attributes

FCS_CKM.1(2) Cryptographic Key Generation (KEK Updates)

Hierarchical to: No other components

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*proprietary algorithm*] and specified cryptographic key sizes [*128 bits*] that meet the following: [*none*].

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_COP.1 Cryptographic operation
FMT_MSA.2 Secure security attributes

FCS_CKM.2 Cryptographic Key Distribution

Hierarchical to: No other components

FCS_CKM.1.2 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*encrypted manual keyfill*] that meets the following: [*none*].

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4(1) Cryptographic Key Destruction (KEK replacement)

Hierarchical to: No other components

FCS_CKM.4.1(1)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*none*].
Dependencies:	FCS_CKM.1 Cryptographic key generation FMT_MSA.2 Secure security attributes
FCS_CKM.4(2)	**Cryptographic Key Destruction (KEK zeroise)**
Hierarchical to:	No other components
FCS_CKM.4.1(2)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*none*].
Dependencies:	FCS_CKM.1 Cryptographic key generation FMT_MSA.2 Secure security attributes
FCS_CKM.4(3)	**Cryptographic Key Destruction (KEK Updates)**
Hierarchical to:	No other components
FCS_CKM.4.1(3)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite or volatile memory release*] that meets the following: [*none*].
Dependencies:	FCS_CKM.1 Cryptographic key generation FMT_MSA.2 Secure security attributes
FCS_CKM.4(4)	**Cryptographic Key Destruction (TEKs)**
Hierarchical to:	No other components
FCS_CKM.4.1(4)	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite or volatile memory release*] that meets the following: [*none*].
Dependencies:	FCS_CKM.1 Cryptographic key generation FMT_MSA.2 Secure security attributes
FCS_COP .1(1)	**Cryptographic Operation (Data encryption/decryption)**
Hierarchical to:	No other components
FCS_COP.1.1(1)	The TSF shall perform [*Data encryption and decryption;* *Cryptographic key exchange*] In accordance with a specified cryptographic algorithm [*AES128*] and cryptographic key sizes [*128 bits*] that meet the following: [*none*].
Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
FCS_COP .1(2)	**Cryptographic Operation (Cryptographic support)**
Hierarchical to:	No other components
FCS_COP.1.1(2)	The TSF shall perform [*Random number generation;* *Initialisation vector generation;* *Initialisation vector exchange*] In accordance with a specified cryptographic algorithm [*proprietary hardware module*] and cryptographic key sizes [*128 bits*] that meet the following: [*none*].

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.2 User Data Protection (FDP)

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components

FDP_IFC.1.1 The TSF shall enforce the [*traffic flow SFP*] on
subjects: the TSF and remote trusted IT products;
information: voice and fax data;
operations: export to the remote trusted IT product].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [*traffic flow SFP*] based on the following types of subject and information security attributes:[*the operator has elected to transmit the information securely*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*a stable communications channel has been established; and the TSF has confirmed that the remote trusted IT product is configured with matching cryptographic settings; and an encrypted channel has been established*].

FDP_IFF.1.3 The TSF shall enforce the [*no additional information flow SFP rules*].

FDP_IFF.1.4 The TSF shall provide the following [*no additional information flow SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules [*none*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules [*none*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components

FDP_UCT.1.1 The TSF shall enforce the [*traffic flow SFP*] to be able to [*transmit*] objects in a manner protected from unauthorised disclosure.

Dependencies: FDP_IFC.1 Subset information flow control
FTP_ITC.1 Inter-TSF trusted channel

5.1.3 Identification and Authentication (FIA)

FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components

FIA_UAU.1.1 The TSF shall allow [
secure session request;
key exchange key update; and
key exchange key selection]
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.7	**Protected Authentication Feedback**
Hierarchical to:	No other components
FIA_UAU.7.1	The TSF shall provide only [*an indication of the number of characters entered*] to the user while the authentication is in progress.
Dependencies:	FIA_UAU.1 Timing of authentication

5.1.4 Security Management (FMT)

FMT_MOF.1	**Management of Security Functions Behaviour**
Hierarchical to:	No other components
FMT_MOF.1.1	The TSF shall restrict the ability to [*determine the behaviour of*] the functions [*encrypt and decrypt data; cipher chaining; manage keys*] to [*the Crypto-Custodian*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_MTD.1(1)	**Management of TSF Data (Cryptographic configuration)**
Hierarchical to:	No other components
FMT_MTD.1.1(1)	The TSF shall restrict the ability to [*query, modify or load*] the [*cryptographic configuration information: cryptographic keys, cryptographic algorithm, and cipher chaining setting, default net*] to [*the Crypto-Custodian*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_MTD.1(2)	**Management of TSF Data (Fax ID)**
Hierarchical to:	No other components
FMT_MTD.1.1(2)	The TSF shall restrict the ability to [*query, modify or load*] the [*fax authentication identifier*] to [*the Administrator or Crypto-Custodian*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_MTD.1(3)	**Management of TSF Data (Crypto-Custodian password)**
Hierarchical to:	No other components
FMT_MTD.1.1(3)	The TSF shall restrict the ability to [*modify*] the [*Crypto-Custodian password*] to [*the Crypto-Custodian*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_MTD.1(4)	**Management of TSF Data (Administrator password)**
Hierarchical to:	No other components
FMT_MTD.1.1(4)	The TSF shall restrict the ability to [*modify*] the [*Administrator password*] to [*the Administrator*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_MTD.1(5)	**Management of TSF Data (KEK selection)**
Hierarchical to:	No other components
FMT_MTD.1.1(5)	The TSF shall restrict the ability to [*modify*] the [*selected KEK number and KEK update cycle number*] to [*the operator*].
Dependencies:	FMT_SMR.1 Security Roles
FMT_SMR.1	**Security Management Roles**
Hierarchical to:	No other components

FMT_SMR.1.1	The TSF shall maintain the roles [*Crypto-Custodian, Administrator and operator*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.3	**Assuming Roles**
Hierarchical to:	No other components
FMT_SMR.3.1	The TSF shall require an explicit request to assume the following roles: [*Crypto-Custodian and Administrator*].
Dependencies:	FMT_SMR.1 Security roles

5.1.5 Protection of the TSF (FPT)

FPT_AMT.1	**Abstract Machine Testing**
Hierarchical to:	No other components
FPT_AMT.1.1	The TSF shall run a suite of tests [*during initial start-up*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
Dependencies:	No dependencies
FPT_ITA.1	**Availability of Exported TSF Data**
Hierarchical to:	No other components
FPT_ITA.1.1	The TSF shall ensure the availability of [*cryptographic key information and session establishment data*] provided to a remote trusted IT product within [*the key exchange process*] given the following conditions: [*a stable communications channel can be established and maintained; and the TSF has confirmed that the remote trusted IT product is configured with matching cryptographic settings*].
Dependencies:	No dependencies
FPT_ITC.1	**Confidentiality of Exported TSF Data**
Hierarchical to:	No other components
FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.
Dependencies:	No dependencies
FPT_ITI.1	**Inter-TSF Detection of Modification**
Hierarchical to:	No other components
FPT_ITI.1.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*HDLC error detection*].
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*error reporting*] if modifications are detected.
Dependencies:	No dependencies
FPT_PHP.3	**Resistance to Physical Attack**
Hierarchical to:	No other components
FPT_PHP.3.1	The TSF shall resist [*physical access*] to [*the processing components of the TSF*] by responding automatically such that the TSP is not violated.
Dependencies:	No dependencies

5.1.6 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*fax authentication identifier of the destination*].

Dependencies: No dependencies

5.1.7 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

FTP_ITC.1.1 The TSF shall provide a communications channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF and the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*exchange of trusted channel setup data*].

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

This section contains the security assurance requirements for the TOE. The requirements are summarised in the table below:

Table 8. TOE Security Assurance Requirements

No.	Component	Component Name
Class ACM: Configuration Management		
1	ACM_CAP.2	Configuration Items
Class ADO: Delivery and Operation		
2	ADO_DEL.1	Delivery Procedures
3	ADO_IGS.1	Installation, Generation and Start-Up
Class ADV: Development		
4	ADV_FSP.1	Informal Functional Specification
5	ADV_HLD.1	Descriptive High-Level Design
6	ADV_RCR.1	Informal Correspondence Demonstration
Class AGD: Guidance Documentation		
7	AGD_ADM.1	Administrator Guidance
8	AGD_USR.1	User Guidance
Class ATE: Tests		
9	ATE_COV.1	Evidence of Coverage

10	ATE_FUN.1	Functional Testing
11	ATE_IND.2	Independent Testing – Sample
Class AVA: Vulnerability Assessment		
12	AVA_SOF.1	Strength of TOE Security Function Evaluation
13	AVA_VLA.1	Developer Vulnerability Analysis

5.2.1 Configuration Management (ACM)

ACM_CAP.2 Configuration Items

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to unique identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Dependencies: No dependencies

5.2.2 Delivery and Operation (ADO)

ADO_DEL.1 Delivery Procedures

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Dependencies: No dependencies

ADO_IGS.1 Installation, Generation and Start-Up

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation and start-up of the TOE.

Dependencies: AGD_ADM.1 Administrator guidance

5.2.3 Development (ADV)

ADV_FSP.1 Informal Functional Specification

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.
Dependencies:	ADV_RCR.1 Informal correspondence demonstration
ADV_HLD.1	**Descriptive High-Level Design**
ADV_HLD.1.1D	The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1C	The presentation of the high level design shall be informal.
ADV_HLD.1.2C	The high level design shall be internally consistent.
ADV_HLD.1.3C	The high level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C	The high level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C	The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware or software.
ADV_HLD.1.6C	The high level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7C	The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
Dependencies:	ADV_FSP.1 Informal functional specification ADV_RCR.1 Informal correspondence demonstration
ADV_RCR.1	**Informal Correspondence Demonstration**
ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representation that are provided.
ADV_RCR.1.1C	For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
Dependencies:	No dependencies

5.2.4 Guidance Documents (AGD)

AGD_ADM.1	**Administrator Guidance**
AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
Dependencies:	ADV_FSP.1 Informal functional specification
AGD_USR.1	**User Guidance**
AGD_USR.1.1D	The developer shall provide user guidance.
AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
Dependencies:	ADV_FSP.1 Informal functional specification

5.2.5 Tests (ATE)

ATE_COV.1	**Evidence of Coverage**
ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification
Dependencies:	ADV_FSP.1 Informal functional specification ATE_FUN.1 Functional testing
ATE_FUN.1	**Functional Testing**
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C	The test results from the developer shall demonstrate that each tested security function behaved as specified.
Dependencies:	No dependencies
ATE_IND.2	**Independent Testing - Sample**
ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
Dependencies:	ADV_FSP.1 Informal functional specification AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance ATE_FUN.1 Functional testing

5.2.6 Vulnerability Assessment (AVA)

AVA_SOF.1	**Strength of TOE Security Function Evaluation**
AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
Dependencies:	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high-level design
AVA_VLA.1	**Developer Vulnerability Analysis**
AVA_VLA.1.1D	The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2D	The developer shall document the disposition of obvious vulnerabilities.
AVA_VLA.1.1C	The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
Dependencies:	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high-level design AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance

5.3 Security Requirements for the IT Environment

There are no additional explicit security requirements for the TOE's IT environment.

5.4 Security Requirements for the non-IT Environment

The following requirements are met by the TOE's non-IT environment:

Table 9. Security Assurance Requirements for the TOE's non-IT Environment

No.	Component	Description
1	ENV_INSTALL	The TOE must be installed and configured in accordance with instructions and administrator guidance provided to the user organisation by the developer.

2	ENV_LOCATE	The non-IT environment provides sufficient controls to ensure the physical security of the TOE.
3	ENV_SECRETS	All sensitive cryptographic material, cryptographic management information and security management information for use with the TOE must be protected physically and procedurally from compromise.
4	ENV_TRAINING	TOE users shall be thoroughly trained in the operation and purpose of the TOE in order to operate the TOE correctly in their allocated role(s).
5	ENV_VET	The user organisation must ensure that all users permitted access to the TOE are trustworthy and are motivated to operate the TOE correctly and in accordance with the user organisation's security policy.

6 TOE Summary Specification

This section describes the security functions and assurance measures of the TOE that allow the TOE security requirements to be met.

6.1 TOE Security Functions

In order to satisfy the SFRs identified in Section 5.1, TOE Security Functional Requirements, the TOE performs the following IT security functions:

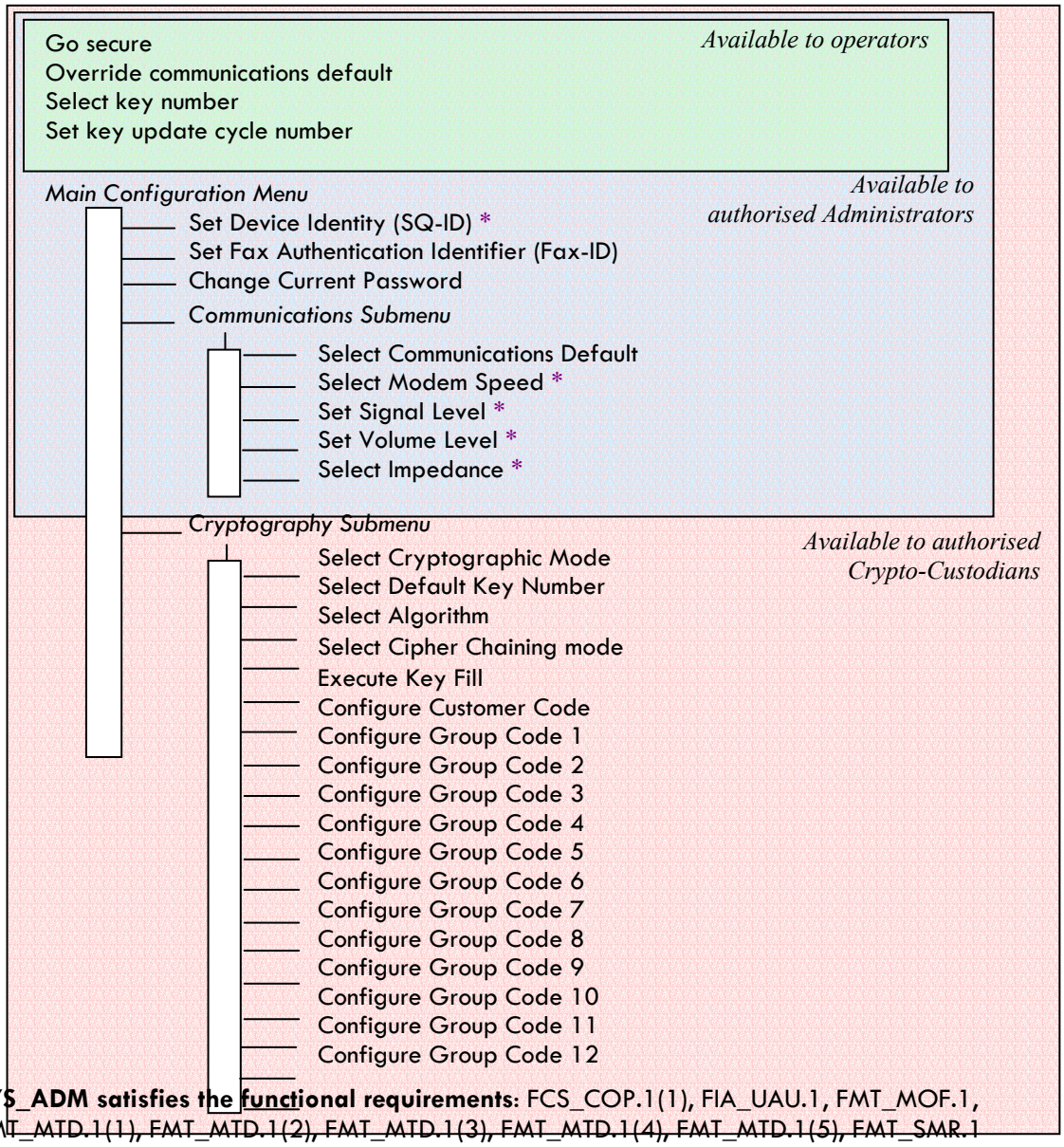
Table 10. TOE Security Functions

Name	Description
System administration (SYS_ADM)	Maintain system configuration information
Authentication and verification (SYS_AUTH)	Authenticate users and validate user actions
System self-testing (SYS_STEST)	Confirm system integrity at start-up
System status feedback (SYS_STATUS)	Confirm system status during operation
Manage TEKs (MK_TEK)	Generate traffic exchange keys for use
Manage KEKs (MK_KEK)	Securely store traffic exchange keys for use
Manage KEK updates (MK_UPDATE)	Derive key exchange key updates for use
Communications session management (F_LINE)	Establish and maintain the communications channel
Secure session management (F_GOSECURE)	Establish security across the communications channel
Encryption/decryption (F_CRY)	Encrypt and decrypt data for voice and fax communications
Tamper response (F_TAMPER)	Detect and respond to violations of physical integrity

6.1.1 System Administration (SYS_ADM)

TOE system management is through a password protected menu system. The TOE supports two passwords offering different levels of access. The Administrator password authorises access to view and modify communications related configuration items. The Crypto-Custodian password authorises the user to access cryptographic configuration items, as well as to all items permitted to an Administrator. A valid password must be entered before the configuration menu can be accessed and the menu will automatically close if no configuration activity is detected for a period of two minutes.

The structure and contents of the configuration system and the privileges assigned at each authorisation level are as follows (items marked * are not TSF-relevant; please refer to administrator guidance documentation for full descriptions of each item):



SYS_ADM satisfies the functional requirements: FCS_COP.1(1), FIA_UAU.1, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5), FMT_SMR.1

6.1.2 Authentication and Verification (SYS_AUTH)

The TOE performs the following authentication and verification actions:

a) an authorisation check when a request is received to access the configuration menu, by comparing the password entered with the Administrator password and Crypto-Custodian password (in that order) to detect a match;

b) a verification check when a request is received to alter a password, to ensure that the user has correctly entered the intended replacement password;

c) an authorisation check when a request is received from a remote SQ-Phoenix to start a secure session by attempting to decrypt the request packet from that equipment with the cryptographic information stored in the TOE;

d) an authorisation check when a request is made to load new cryptographic key material, by requiring the key table to include the same Customer Code as the TOE, and for the entire key table to be encrypted with the same encryption key as exists in the TOE to decrypt the key table;

e) an authorisation check when a request is made to load new cryptographic key material, by requiring the fill device operator to enter an authorisation code matching one used when the fill device was loaded;

f) an integrity check when a request is made to load new cryptographic key material, by requiring that a checksum generated when the key material file was loaded into the fill device matches the checksum generated at the TOE when the key material file is transferred to the TOE.

g) an authentication check when a request is made to send a secure fax, to confirm that the destination device is the intended recipient;

Feedback is returned to the operator in response to each of these checks as follows:

a) If the authorisation check passes, the operator is granted access to the configuration menu.
If the authorisation check fails, no error message is returned and the TOE returns to the idle state.

b) If the verification check passes, the configuration menu moves to the next configuration item.
If the verification check fails, the following error message is returned:

   i) PASSWORD FAIL 50 – non-identical change and confirm entries for new password

c) If the authorisation check passes, a secure session is established.
If the authorisation check fails, one of the following error messages is returned:

   i) CRYPTO FAIL 11 – not authorised

   ii) CRYPTO FAIL 12 – unable to verify authorisation

d) If the authorisation check passes, the key fill process continues.
If the authorisation check fails, the following error message is returned:

   i) KEYFILL FAIL 53 – not authorised

e) If the authorisation check passes, the key fill process continues.
If the authorisation check fails, the following error message is returned:

   i) KEYFILL FAIL 53 – not authorised

f) If the authorisation check passes, the key fill process continues.
If the authorisation check fails, the following error message is returned:

   i) KEYFILL FAIL 52 – integrity violation

g) If the authentication check passes, the transmission process continues.
If the authentication check fails, the following error message is returned:

   i) COMMS FAIL 16 – fax authentication failure

6.1.2.1 Strength of Function

The security functions outlined in (a), (e) and (g) are probabilistic and have Strength of Function SOF-basic. The security function in (d) is probabilistic and has Strength of Function SOF-high. The strength of each security function is calculated below, with reference back to the descriptions in section 6.1.2.

(a) Password

When the password is entered to request access to the configuration menu, the values are displayed as asterisks to prevent unauthorised disclosure of the password to any party observing the feedback display. The password is checked after it has been entered in total and the operator has pressed SET; in the event of an authentication failure, no indication is given of which digit(s) do not match a valid password. In the event of the two passwords being identical, only the Administrator level is accessible. Each password must be between one and eight digits in length, and the TOE Administrator Guidance recommends that passwords be eight digits in length. Passwords can only be entered via the keyboard.

The probability of any one attempt to guess an authorised password granting access to any configuration items is 0.00000002 (two in one hundred million). There is no limitation on the number of attempts which may be made. Each attempt fails or is accepted immediately. The time required per attempt is approximately three seconds. A brute force attempt to manually gain configuration access would take on average 868 days to succeed (20 tries per minute at 100,000,000 combinations = 5,000,000 minutes to attempt all possible combinations; two possibilities for access and length to break calculated at 50% of all possibilities = ((5,000,000 ÷ 2) ÷ 2) = 1,250,000 minutes (20,833.333 hours, 868.055 days).

Cracking a password and gaining access to configuration data would allow the attacker to modify certain operating parameters. In the event of Crypto-Custodian access being gained, the attacker could change the TSF operating settings to electronic codebook, instead of cipher feedback, or to use the system algorithm instead of AES128, or could corrupt the configured cryptographic keys. Any of these actions would prevent an operator communicating successfully with other operators. Identifying a password would not give the attacker access to sensitive information or sensitive cryptographic material as the TOE does not support export of sensitive cryptographic information to any user.

(d) Keyfill authorisation code (Valid key table)

In order to load an unauthorised keyset into the TOE, the attacker would have to determine the Customer Code and transfer key stored in the SQ-Phoenix, generate a key table using this information, and gain access to the TOE's cryptography submenu in order to load the new keyset (please see calculations in paragraph (e) below). The Customer Code is 16 decimal digits in length and the transfer key is 128 bits. At a total of 3.403×10^{54} combinations, this is not considered feasible to break under a brute force attack.

(e) Keyfill authorisation code (Operator authorisation)

Access to the keyfill operation is restricted to Crypto-Custodians. Authentication is password based and may be calculated as in paragraph (a) above, but there is only one correct answer in the 100,000,000 possibilities so the time required would double.

The authorisation code is four digits and there is no limitation on the number of attempts which may be made. Each attempt is accepted or fails after the new key table has been decrypted and checked. If the keyfill fails there is a 5 second error message display; the time required per attempt is thus approximately seven seconds. A brute force attempt to determine the authorisation code to execute the keyfill process would take on average 10 hours to succeed (8.57 tries per minute at 10,000 combinations = 1166.667 minutes to attempt all possible combinations; one correct code and length to break calculated at 50% of all possibilities = 583.333 minutes (9.72 hours).

Determining the authentication code would permit an attacker who has gained access to the cryptographic configuration menu to load a keyset which had been generated for use within the network. This could result in an operator using a different keyset from the one currently in use throughout the network, preventing the operator from communicating securely with others in the network until the TOE could be reconfigured. The change could not be hidden so the level of protection provided by the TSF could not be silently lowered. This action would have mainly nuisance value.

(g) Fax authentication identifier.

The Fax ID permits a fax transmission to be designated by the sender as destined for a particular recipient, identified by the Fax ID stored in the receiving SQ-Phoenix. If the Fax ID entered for the transmission does not match the stored code, the receiving unit rejects the incoming document before the

cryptographic session is initiated and the sender receives an error notification COMMS FAIL 16. The Fax ID may be up to four digits and the code requested must exactly match the stored code. Even if the Fax ID of the intended recipient could be determined, an attacker would still have to program the false unit with appropriate keys to permit the transmission to continue.

The probability of an unauthorised SQ-Phoenix being programmed with the correct Fax ID to accept an incoming fax destined for another unit (assuming the telephone line could be diverted to the false unit) is one in ten thousand (0.0001). An attacker attending the false unit could change the Fax ID between transmission attempts by the sender, but it is considered unlikely that a sender would attempt more than 10 transmissions before calling the intended recipient to confirm operability of the intended destination unit, thereby discovering the presence of the attacker. The probability of successfully guessing a Fax ID and gaining access to a transmission is therefore estimated to be ten in ten thousand, or 0.001. This is consistent with SOF-basic.

SYS_AUTH satisfies the functional requirements: FCS_CKM.1(2), FCS_CKM.2, FCS_COP.1(1), FDP_IFF.1, FIA_UAU.1, FIA_UAU.7, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_SMR.1, FMT_SMR.3,FPT_ITA.1, FTA_TSE.1

6.1.3 System Self-Testing (SYS_STEST)

The TOE automatically performs the following self-test actions:

a) a self-test at start-up to confirm correct functioning of hardware components;

b) a self-test at start-up to check that the software and configuration settings have not been corrupted.

Feedback is returned to the operator in response to each of these checks as follows:

a) If the self-test passes, the unit initialises to the idle state
If the unit fails, one of the following error messages is returned:

   i) CRYPTO FAIL 44 – error initialising cryptographic co-processor

   ii) ST75 FAIL 41 – error initialising vocoder chip (coder)

   iii) ST75 FAIL 42 – error initialising vocoder chip (decoder)

   iv) ST75 FAIL 43 – error initialising line modem

   v) EEPROM FAIL 30 – unable to read EEPROM

b) If the self-test passes, the unit initialises to the idle state
If the unit fails, the following error message is returned:

   i) EEPROM FAIL 30 – mismatch between EEPROM data and last calculated checksum

SYS_STEST satisfies the functional requirements: FPT_AMT.1

6.1.4 System Status Feedback (SYS_STATUS)

The TOE includes precise feedback messages to provide the operator with relevant and useful information regarding the current operating status of the unit, and to assist in identifying the cause in the event of any failure (system, authentication or communications).

A comprehensive list of messages for SYS_STATUS is contained in the Administrator Guidance documentation.

SYS_STATUS satisfies the functional requirements: FIA_UAU.7, FPT_AMT.1, FPT_ITI.1

6.1.5 Manage key encrypting keys (MK_KEK)

The TOE uses externally generated key encrypting keys (KEKs) to encrypt the session unique traffic exchange keys during key exchange. The TOE needs to accept these keys from the Crypto-Custodian, verify them as genuine, store them securely and destroy them when superseded.

The TOE accepts and verifies the KEKs under the Keyfill process.

For the Keyfill process to succeed, the attacker requires knowledge of the TOE's Crypto-Custodian password and keyfill authorisation code, as well as having physical access to the TOE. The key table

must include the TOE's Customer Code and the key configured in the TOE to encrypt and decrypt the key table. Crypto-Custodians are trusted, and the user organisation has been assumed to be operating a rigorous programme of physical security around its key generation facility. An attacker would therefore need to determine all of the information by interception and cryptanalysis, or by guesswork. The quality of the sensitive cryptographic material generated by the user organisation is outside the scope of the evaluation and has been assumed at SOF-high.

In order to load an unauthorised keyset into the TOE, the attacker would have determine the Customer Code and transfer key stored in the SQ-Phoenix. The Customer Code is 16 decimal digits in length and the transfer key is 128 bits. At a total of 3.403×10^{54} combinations, this is not considered feasible to break under a brute force attack.

The KEKs are stored in secured EEPROM memory within the TOE, protected by hardware security locks, and are retrieved into volatile RAM at the start of a secure session negotiation. The KEK is cleared from RAM as soon as the negotiation phase is complete, or when overwritten by the update process. The KEKs cannot be read back from the TOE, nor does the TOE support export of the KEKs to any user.

The TOE destroys superseded KEKs by overwriting them with new key material. The TOE does not support validity periods and automatic invalidation of key material. KEKs are also cleared from EEPROM when an emergency erase function is activated, or when zeroised by a factory reset.

The KEKs are encrypted throughout the keyfill process and are only decrypted once data integrity has been confirmed and the key table has been stored within the TOE. The KEKs are not vulnerable to disclosure while stored in the fill device or during the keyfill process.

The default operating KEK may only be set by the Crypto-Custodian. The default KEK setting may be overridden by the operator on a per-session basis; the operator may only successfully communicate using a selected KEK if that KEK has been configured by the Crypto-Custodian with valid data.

6.1.5.1 Strength of Function

The SOF value of MK_KEK is assessed as SOF-high.

MK_KEK satisfies the functional requirements: FCS_CKM.2, FCS_CKM.4(1), FCS_CKM.4(2), FDP_IFF.1

6.1.6 Manage traffic exchange keys (MK_TEK)

The TOE includes a mechanism for generating random numbers which are used as traffic exchange keys. The random number generator (RNG) contains a random generation mechanism plus a means of converting the random information into a usable form. The generating mechanism is a high speed single ring oscillator, and its random output is aggregated into a 32 bit word within the RNG processor; four words are provided to produce the 128 bit traffic key and the 128 bit session IV.

A new TEK and IV are generated at the start of each secure session and the encryption and decryption keys are stored in non-volatile memory until overwritten by TEKs for a new session, or cleared from memory when power is removed. The IV is constantly overwritten during a session as well as at the start of each session or when power is removed.

6.1.6.1 Strength of Function

The security of cryptographic keys is critical to the overall strength of the TSF and the SOF value of MK_TEK is assessed as SOF-high.

Frequency (Monobit test)

The focus of the test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same. This test was successfully completed for streams from 100 to 7,900,000 bits.

Runs Test

The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the

number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow. This test was successfully completed for streams from 100 to 7,900,000 bits.

Binary Matrix Rank Test

The purpose of this test is to check for linear dependence among fixed length substrings of the original sequence. This test was run for a 32 x 32 bit substring matrix, and was successfully completed for streams from 38,912 to 7,900,000 bits.

Cumulative Sums (Cusum) Test

The purpose of the test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behaviour of that cumulative sum for random sequences. This cumulative sum may be considered as a random walk. For a random sequence, the excursions of the random walk should be near zero. For certain types of non-random sequences, the excursions of this random walk from zero will be large. The test was run in both forwards and backwards walk modes, and was successfully completed for streams from 100 to 7,900,000 bits.

MK_TEK satisfies the functional requirements: FCS_CKM.1(1), FCS_CKM.4(4), FCS_COP.1(2), FDP_IFF.1

6.1.7 Manage key encrypting key updates (MK_UPDATE)

The TOE includes an algorithm which is used to generate pseudo-random output. This is used for the KEK "update" generation process, which allows the keys loaded into the TOE by the Crypto-Custodian to be expanded into a larger set, allowing key changes to be scheduled more frequently.

A pseudo-random algorithm is required for this process because the output must be identical for all equipment within a network in order to retain secure compatibility. The algorithm is seeded by one of the 128 bit net keys stored in the TOE and the algorithm is exercised for a number of repetitions defined by the configured update number (to a maximum of 99 times).

The KEK Update is stored in non-volatile memory and is cleared from memory when power is removed, or overwritten by another Update for a new session.

The KEK Update process is managed by the operator via the TOE's keypad.

6.1.7.1 Strength of Function

The security of cryptographic keys is critical to the overall strength of the TSF and the SOF value of MK_UPDATE, based on initial cryptographic keys produced by the user organisation to SOF-high, is assessed as SOF-high.

Random numbers are created using a recursive formula. The pRNG is a 32 bit algorithm so the 128 bit KEK is split into four parts, and each part is used in turn to seed the pRNG. Starting with a 32-bit seed value S1 (i.e., a positive number in the range 0…232-1), a new number S2 is created using the formulae:

$X = S1 \times M + 1$ where M is the RNG Multiplier = 22,695,477

$S2 = high32(X)\ XOR\ low32(X)$

The 64-bit number X resulting from the first step is split into two 32-bit parts, which are exclusive-or'd together to form the new S2 value for use in the next iteration of the formula. The random number generated from this iteration is the S2 value.

The random numbers are close to optimal in the Momentum tests. The first moment, the Arithmetic Mean, is the sum of measurements divided by the number of measurements in the set. The optimal value for a uniform distribution is 127.5 and the pRNG gives a value of 126. The second moment, Variance, is a measure of the dispersion of random numbers about the mean. If these values are centred around the mean the variance is small; if they are far from the mean it is large. For a uniform distribution, the ideal variance is 5461. The pRNG gives a value of 5516. The third moment, Skewness, is a measure of the asymmetry of the distribution. If the values are distributed more to the right of the mean the skewness is positive, if to the left, negative. For a uniform distribution, the ideal skewness is zero. The pRNG gives a value of .0073 for Skewness. Kurtosis, the fourth moment, is a measure of the

peakedness of the distribution. For a uniform distribution the ideal kurtosis is 1.8. The pRNG gives a kurtosis value of 1.78.

Frequency/Serial tests can be used to measure the flatness and randomness of the numbers generated through an RNG. The frequency test is a measure of the uniformity of successive sets of numbers and is performed using the Chi-Square goodness-of-fit test. The serial test measures the degree of randomness between successive numbers. The ideal range of results for the two tests combined is from 233 to 275. The pRNG results in a value of 233.3.

The Poker test is also used to test the randomness of an RNG. This test looks for the occurrences of no two consecutive values the same, or any two values the same, three values the same or four values the same. The values produced on analysis of the pRNG, compared to optimal values (in brackets), are 1271 (1365), 625 (630), 81 (52.5), and 1 (0.5).

MK_UPDATE satisfies the functional requirements: FCS_CKM.1(2), FCS_CKM.4(3), FDP_IFF.1

6.1.8 Communications Session Establishment and Maintenance (F_LINE)

The TOE is a digital encryptor and as such its output is a bitstream. For this to be accurately conveyed across the analog communications medium, the TOE supports a method of digital communications based on the V32.bis modem standard.

Data is sent across the communications channel in 19-byte blocks, transmitted as packets of 8, 8 and 3 bytes. Each packet carries a checksum which is used for error detection. If an error is detected during key exchange, the key exchange process fails and returns the message CRYPTO FAIL 12. If an error is detected during the body of the transmission, the packet is discarded; errors are not accumulated across packets. A high proportion of line errors reduces the perceived quality of the received signal.

F_LINE satisfies the functional requirements: FDP_IFF.1, FPT_ITA.1, FPT_ITI.1

6.1.9 Secure session establishment (F_GOSECURE)

The TOE establishes a secure communication session with a remote trusted SQ-Phoenix by exchanging data across a digital connection which can only be successfully interpreted and responded to if the remote equipment has identical cryptographic information available. The TOE expects and must successfully recover a byte value in a fixed location in the first encrypted packet of the key exchange. The process may be initiated by the local user or the remote trusted IT product.

If the secure session cannot be established, the TOE returns a CRYPTO FAIL 11 error message (non-matching cryptographic configuration).

Secure session establishment requires a stable communications connection to be established first, then security information is exchanged across this channel.

6.1.9.1 Strength of Function

The strength of the protection provided by the traffic encryption is dependent on the strength of protection provided by the securing process as a weak F_GOSECURE would allow simple TEK recovery and the entire secure session would be compromised. The security of F_GOSECURE depends on two main components: the strength of the KEKs generated by the customer and installed in the TOE; and the strength of the algorithm which is used in conjunction with those KEKs (or their derivative updates) to encrypt the secure session packets. The strength of the customer KEKs is assumed as SOF-high; the strength of derivative updates is assessed under MK_UPDATE as SOF-high; the algorithm used in F_GOSECURE is the AES128 algorithm in electronic codebook mode, which is assessed as SOF-high. The overall strength of F_GOSECURE is assessed as SOF-high.

F_GOSECURE satisfies the functional requirements: FCS_COP.1(1), FCS_COP.1(2), FDP_IFF.1, FIA_UAU.1, FPT_ITA.1, FPT_ITC.1, FTP_ITC.1

6.1.10 Encryption/decryption for voice and fax communications (F_CRY)

The TOE performs digital encryption processes on fax data and digitised voice signals, using the AES128 algorithm and 128 bit keys, and cipher feedback (CFB) mode of operation. CFB is a stream cipher method, whereby data from the encryption process is XORed from the plaintext and the result of this process is sent to the line for transmission. CFB provides additional security over the ECB block ciphering method because in effect the TEK is constantly changed throughout the session.

6.1.10.1 Strength of Function

Traffic encryption is the core security function of the TOE and is affected by two factors: the strength of the algorithm and the strength of the KEKs. As such, the SOF value of F_CRY is dependent on the assessed SOF value of MK_TEK and F_GOSECURE. The overall strength of F_CRY is assessed as SOF-high.

F_CRY satisfies the functional requirements: FCS_COP.1(1), FDP_IFC.1, FDP_UCT.1

6.1.11 Tamper Response (F_TAMPER)

The TOE has zeroisation circuitry which allows sensitive cryptographic key material to be erased when the TOE's security is compromised. The compromise may be an actual attempt to violate the TOE's physical integrity (tampering) or may be an incipient threat of breach of physical security, detected by the operator and acted upon by deliberately zeroising critical information. Both mechanisms operate by overwriting zeroes to memory locations assigned to key material. The physical mechanism for tamper-detect is a microswitch in the main circuitry which is held closed by a small post on the inside of the TOE's case; the operator action zeroise (emergency erase) switch is a recessed switch at the rear of the device.

In the absence of an external power supply, the emergency erase and anti-tamper systems are powered by the TOE's internal battery.

F_TAMPER satisfies the functional requirements: FPT_PHP.3

6.2 Assurance Measures

The TOE claims to satisfy assurance requirements to CC EAL2. The following assurance measures are applied to satisfy the SARs identified in Section 5.2, TOE Security Assurance Requirements:

Table 11. TOE Security Assurance Measures

Name	Description
Configuration Management	Methodology and documentation tracking versions of the TOE and its components
Safe Delivery Procedure	Methodology and documentation to ensure security of the TOE in transit
Safe Configuration and Installation Directions	Documentation supporting correct installation of the TOE
Development Documentation	Technical documentation describing the TOE's functional and assurance security profile and analysing the TOE's abstract form
User Guidance	Guidance documentation for users of the TOE
Test Procedures	System, procedures and documentation to ensure the correct and consistent operation of the TOE
Vulnerability Assessment	Analysis of the security strength and potential vulnerabilities of the TOE

6.2.1 Configuration Management

CES has identified a list of engineering, documentation and support components involved in each instance of the TOE, and each component is identified by a unique product identifier. These unique identifiers are updated to reflect each new release of the TOE.

These configuration measures are documented in a configuration management list, embodied in the following document:

- CES03/32 – SQ-Phoenix Configuration Management System

6.2.2 Safe Delivery Procedure

Guidelines have been developed to ensure that the TOE can be delivered to end users with a high level of confidence that the equipment has not been interfered with. These guidelines include directions on the packing and despatch procedure, instructions for distribution agents, and guidance for the customer when receiving instances of the TOE.

These guidelines are embodied in the following documents:

- CES03/40 – SQ-Phoenix Shipment and Delivery Procedure
- CES03/41 – SQ-Phoenix Delivery Acceptance
- CES03/42 – SQ-Phoenix Battery Connection and Seal Fixing
- SQ-Phoenix Installation and Start-Up Guide

6.2.3 Safe Configuration and Installation Directions

Additional guidelines are provided for the user organisation to ensure that once the TOE has been safely received, it can be correctly configured and installed to permit it operate in the intended manner. Directions are also give on configuring the equipment to the TOE configuration, to reduce the risk of inadvertent installation of SQ-Phoenix units outside the evaluated configuration.

These guidelines are embodied in the following documents:

- SQ-Phoenix Operating Manual
- SQ-Phoenix Installation and Start-Up Guide

6.2.4 Development Documentation

CES has documented the design, specifications and interfaces of the TOE in a series of publications., A functional specification, in an informal style, describes the TSF's external interfaces, with details of TOE responses to user actions, and relates these interfaces to the TOE security functions. A high level design provides an overview of the TSF in terms of subsystems, and relates these subsystems to the functions and interfaces.

These guidelines are embodied in the following documents:

- CES03/31 – SQ-Phoenix Security Target
- CES03/33 – SQ-Phoenix Functional Specification
- CES03/34 – SQ-Phoenix High-Level Design

6.2.5 User Guidance

Detailed guidance is provided for users to ensure the TOE is used as intended, to provide the claimed functionality. Separate guidance is provided for users with Crypto-Custodian privileges, who will take responsibility for configuring the TOE to operate correctly and efficiently.

The user guidance is embodied in the following documents:

- SQ-Phoenix Operating Manual
- SQ-Phoenix Installation and Start-Up Guide
- SQ-Phoenix User Guide

6.2.6 Test Procedures

The suite of test documentation includes test plans and procedures, together with a record of the actual performance of the TOE compared to the expected results. The TOE is also independently tested by the evaluator as part of the evaluation.

The purpose, manner and procedures for functional testing of the TOE are documented in:

- CES03/10 – SQ-Phoenix Quality Plan
- CES03/36 – SQ-Phoenix Test Plan
- CES03/19 – Quality Testing – SQ-Phoenix - Release v2.x

The actual test results have been supplied on record 030272/192 of CES03/19.

The developer has also supplied equipment to the evaluator to support independent evaluation of the TOE.

6.2.7 Vulnerability Assessment

The developer is required to assess the strength of probabilistic TOE security functions, and seek out and document obvious and exploitable vulnerabilities.

This information is embodied in the following documents:

- CES03/35 – SQ-Phoenix Vulnerability Assessment

7 Protection Profile Claims

The SQ-Phoenix does not claim conformance with any Protection Profiles.

8 Rationale

8.1 Security Objectives Rationale

The security objective rationale shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

The security objective rationale shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

Section 8.1.1, Sufficiency of the Security Objectives, demonstrates that all secure usage assumptions, threats to security and organisational security policies presented in Section 3, TOE Security Environment, are met by at least one Objective as outlined in Section 4, Security Objectives, and justifies the relations in each case. Section 8.1.2,

Correspondence of the Security Objectives, demonstrates that each Objective is required by at least one aspect of the security problem and shows the mapping between the Objectives and the assumptions, threats and policies.

The Security Objectives are necessary and sufficient to satisfy the Security Environment.

8.1.1 Sufficiency of the Security Objectives

Table 12. The Security Objectives meet the Assumptions, Threats and Policies

Security Problem	Security Objective(s)	Justification
A.ADMIN_TRUSTED	OE.INSTALL OE.TRAIN OE.VET	OE.VET ensures that Administrators and Crypto-Custodians are trustworthy and are not motivated to undermine the TSF. OE.TRAIN gives the Crypto-Custodian the ability to configure the TOE soundly and OE.INSTALL ensures that configuration and installation will be completed correctly.
A.ASSET	O.CONFIDENTIALITY	O.CONFIDENTIALITY ensures that the TOE is deployed for the purpose for which it was designed.
A.BYPASS	O.REPORT_STATUS_CRYPTO OE.EDUCATE OE.LOOK_FIRST	OE.EDUCATE is fundamental to ensuring operator awareness of the TOE's operating characteristics and the necessity to decide on the correct operating mode for each situation. OE.LOOK_FIRST ensures that operators do not enter into a communications situation which may compromise the sensitive information. O.REPORT_STATUS_CRYPTO ensures that detailed information on the current security state is available for the operator throughout operation.
A.COMPARTMENTALISE	O.ACCESS_CONTROL O.COMPARTMENTALISE OE.MANAGE_PASSWORDS	O.COMPARTMENTALISE allows compartmentalisation to be translated into the TOE by selectively loading subsets of the user organisation's key materials, which translates into cryptographic keys for designated operating groups. OE.MANAGE_PASSWORDS and O.ACCESS_CONTROL prevents this compartmentalisation being accidentally or deliberately subverted.
A.EMR	O.CONFIDENTIALITY	O.CONFIDENTIALITY ensures that sensitive information is protected when communicated via the TOE.
A.KEYMAN_EXT	O.BLACK_TRANSFER	OE.MANAGE_KEYS addresses the requirement to

	OE.MANAGE_KEYS	ensure that the sensitive cryptographic material prepared for use in the TOE does not compromise the TSF strength of function. O.BLACK_TRANSFER ensures that the security of the key material is not compromised during transfer to the TOE.
A.LOCATE	OE.INSTALL OE.VET	OE.VET and OE.INSTALL ensure that only trusted individuals have access to the TOE.
A.USER_TRUSTED	OE.EDUCATE OE.LOOK_FIRST OE.VET	OE.VET ensures that Operators are trustworthy and are not motivated to undermine the TSF. OE.EDUCATE ensures that Operators are aware of the purpose of the TOE and its operating characteristics. Awareness of the environmental security issues means that appropriately trained Operators can be trusted not to act in a manner which will compromise the TOE's security. OE.LOOK_FIRST ensures that Operators will check that the TOE's configuration supports their intended use before using it to pass sensitive information.
T.ABUSE	O.ACCESS_CONTROL O.COMPARTMENTALISE O.REPORT_STATUS_CRYPTO O.SECRET_KEY_STORE O.STORE_SECURE OE.INSTALL OE.MANAGE_PASSWORDS OE.TAMPER_EVIDENT OE.VET	OE.VET ensures that Operators do not have nefarious intentions in their use of the TSF. O.COMPARTMENTALISE and O.ACCESS_CONTROL allow the Operator's legitimate access rights to be encoded within the TOE's configuration and OE.MANAGE_ PASSWORDS ensures the passwords used for this are robust. OE.INSTALL ensures that the TOE is installed into an appropriate location, so attackers should not have ready physical access to the equipment. O.STORE_SECURE and O.SECRET_KEY_STORE ensure that sensitive cryptographic material is not available from the TOE to any user and can only be accessed at the key management centre. OE.TAMPER_ EVIDENT and O.REPORT_STATUS_CRYPTO allow detection of efforts to access the sensitive cryptographic material or to subvert the TOE.
T.CAPTURE_CRYPTO	O.SECRET_KEY_EXCHANGE	O.SECRET_KEY_EXCHANGE counters the threat by ensuring that successful information interception will not make sensitive cryptographic information available to the attacker.
T.CAPTURE_INFO	O.CONFIDENTIALITY O.SECRET_KEY_EXCHANGE	O.CONFIDENTIALITY removes the risk of the sensitive information being directly available in the event of successful information capture by an attacker. O.SECRET_KEY_EXCHANGE ensures that the attacker cannot gain access to cryptographic session material to enable recovery of the sensitive information.
T.CRACK	O.SECRET_KEY_EXCHANGE OE.MANAGE_KEYS	O.SECRET_KEY_EXCHANGE ensures that sensitive cryptographic material is not readily available through interception. OE.MANAGE_KEYS ensures that key exchange key material is of sufficiently high quality to protect session traffic key

		material.
T.EXTRACT	O.SECRET_KEY_STORE O.STORE_SECURE OE.EDUCATE OE.TAMPER_EVIDENT	O.STORE_SECURE ensures that stored sensitive cryptographic information does not leave the TOE. O.SECRET_KEY_STORE ensures that brute force physical access methods will not succeed in recovering the stored sensitive cryptographic information. OE.EDUCATE and OE.TAMPER_EVIDENT ensure that the user is able to detect an attempt to gain such access to the sensitive cryptographic information.
T.HARDWARE_FAIL	O.REPORT_STATUS_SESSION O.REPORT_STATUS_SYSTEM OE.EDUCATE	O.REPORT_STATUS_SYSTEM counters the threat by ensuring that the operator is apprised of the system's integrity at start-up, or is made aware of any system-related failures. O.REPORT_STATUS_SESSION ensures that the operator is made immediately aware of any integrity failures that may affect successful. communications while a session is in progress. OE.EDUCATE ensures the operator understands these warnings and will take appropriate action to avoid a breach of the TOE.
T.WRONG_FAX	O. AUTHENTICATE_RECIPIENT O.COMPARTMENTALISE O.CONFIDENTIALITY	O.CONFIDENTIALITY allows the document to be sent securely to the authorised recipient. O.COMPARTMENTALISE allows the authorisation of the recipient to be encoded in the choice of cryptographic key; and O.AUTHENTICATE_RECIPIENT allows the intended recipient to be identified with a specific configured instance of the TOE.
TE.ADMIN_ERROR	O.REPORT_STATUS_CRYPTO O.REPORT_STATUS_SESSION OE.INSTALL OE.LOOK_FIRST OE.TRAIN	OE.TRAIN and OE.INSTALL address the threat of human error causing the TOE to be incorrectly configured for use. OE.LOOK_FIRST ensures that in the event of a configuration error, the operator will be aware of the situation and can take corrective action. O.REPORT_STATUS_CRYPTO and O.REPORT_STATUS_SESSION ensure that any activity which alters the operating characteristics of the TOE is detected by the operator at the soonest possible juncture and the sensitive information is not compromised.
TE.INSTALL	OE.TRAIN OE.INSTALL	OE.TRAIN ensures that the individuals responsible for configuring and installing the TOE are trained in the TOE's configuration and operation to the extent that they are able to configure it correctly. OE.INSTALL ensures that this understanding is applied when the TOE is configured and installed.
TE.UNAUTHORISED	OE.INSTALL OE.VET	OE.VET ensures that operators can be trusted and are not motivated to abuse the TSF. OE.INSTALL ensures that the TOE is installed into a location consistent with its design, and that physical controls are in place to ensure that only authorised operators can gain access to the equipment.

P.CONFIDENTIALITY	O.CONFIDENTIALITY OE.INSTALL OE.MANAGE_KEYS OE.TRAIN OE.VET	O.CONFIDENTIALITY ensures that the TOE has the functionality to meet the confidentiality requirement. OE.VET ensures that individuals are trustworthy to use the TOE to protect sensitive information met; OE.TRAIN ensures that Administrators and Crypto-Custodians are appropriately trained in order to support the TOE and its users. OE.INSTALL ensures the TOE is installed correctly to allow it to perform the required security functions. OE.MANAGE_KEYS ensures adequate key quality and handling processes.
P.CRYPTO	O.BLACK_TRANSFER OE.MANAGE_KEYS OE.TRAIN OE.VET	OE.VET ensures that only trustworthy individuals have access to sensitive cryptographic material at any time. OE.TRAIN ensures that Crypto-Custodians understand their role and are capable of performing it correctly. OE.MANAGE_KEYS and O.BLACK_TRANSFER ensure adequate key quality and that this quality is not undermined by handling processes or vulnerability during transfer.
P.PASSWORDS	OE.MANAGE_PASSWORDS OE.TRAIN OE.VET	OE.MANAGE_PASSWORDS ensures that procedures are in place to assure the quality and sound management of passwords. OE.TRAIN ensures administrators are enabled to operate the TOE correctly in execution of their duties; OE.VET ensures administrators are trusted to operate the TOE responsibly.

8.1.2 Correspondence of the Security Objectives

The correspondence table below shows that all aspects of the security environment are met by at least one security objective, and each security objective is necessary to meet at least one aspect of the security environment.

Table 13. Correspondence Table for the Security Objectives

	O.ACCESS_CONTROL	O.AUTHENTICATE_RECIPIENT	O.BLACK_TRANSFER	O.COMPARTMENTALISE	O.CONFIDENTIALITY	O.REPORT_STATUS_CRYPTO	O.REPORT_STATUS_SESSION	O.REPORT_STATUS_SYSTEM	O.SECRET_KEY_EXCHANGE	O.SECRET_KEY_STORE	O.STORE_SECURE	OE.EDUCATE	OE.INSTALL	OE.LOOK_FIRST	OE.MANAGE_KEYS	OE.MANAGE_PASSWORDS	OE.TAMPER_EVIDENT	OE.TRAIN	OE.VET
A.ADMIN_TRUSTED													X					X	X
A.ASSET					X														
A.BYPASS						X						X		X					
A.COMPARTMENTALISE	X			X												X			
A.EMR					X														
A.KEYMAN_EXT			X												X				
A.LOCATE													X						X
A.USER_TRUSTED												X		X					X
T.ABUSE	X			X		X				X	X		X			X	X		X
T.CAPTURE_CRYPTO									X										
T.CAPTURE_INFO					X				X										
T.CRACK									X						X				
T.EXTRACT										X	X	X					X		
T.HARDWARE_FAIL							X	X				X							
T.WRONG_FAX		X		X	X														
TE.ADMIN_ERROR						X	X						X	X				X	
TE.INSTALL													X					X	
TE.UNAUTHORISED													X						X
P.CONFIDENTIALITY					X								X		X			X	X
P.CRYPTO			X												X			X	X
P.PASSWORDS																X		X	X

8.2 Security Requirements Rationale

The security requirements rationale shall demonstrate that the set of security requirements (functional and environment) is suitable to meet and traceable to the security objectives.

8.2.1 Necessity and Sufficiency of the Security Requirements

Each security objective as outlined in Section 4, Security Objectives, is related to at least one security requirement; each requirement is required by at least one Objective. The mapping between these two facets and the justification for the relationship in each case is shown in the table below. The security requirements are necessary and sufficient to satisfy the Security Objectives.

Table 14. The Security Requirements satisfy the Security Objectives

Security Objective	Security Requirement	Justification
O.ACCESS_CONTROL	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) FMT_SMR.1 FMT_SMR.3 FIA_UAU.1 FIA_UAU.7	FMT_MOF.1, FMT_MTD.1, FMT_SMR.3 and FIA_UAU.1 prevent an operator from altering the profile of privileges by requiring authentication to the Crypto-Custodian level before security parameters can be altered. FIA_UAU.7 prevents an operator or Administrator gaining access to Crypto-Custodian authentication information by observing the authentication of a legitimate Crypto-Custodian. FMT_SMR.1 is a dependency of FMT_SMR.3.
O. AUTHENTICATE_RECIPIENT	FCS_COP.1(1) FMT_MTD.1(2) FTA_TSE.1	FCS_COP.1(1) ensures that a document containing sensitive information can be transmitted securely only to another authorised user. FTA_TSE.1 provides the mechanism for restricting the recipient of a document to the operator of a specified remote trusted IT product. FMT_MTD.1(2) ensures that the authentication data can only be changed by authorised personnel.
O.BLACK_TRANSFER	FCS_CKM.2	FCS_CKM.2 ensures that the distribution of sensitive cryptographic material is conducted in a secure manner.
O.COMPARTMENTALISE	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(5)	These requirements enable the administrator to restrict an operator's access to sensitive information by encoding access privileges and restrictions in the TOE's operating configuration, and enable the operator to communicate within the authorised grouping.
O.CONFIDENTIALITY	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.2 FCS_CKM.4(1) FCS_CKM.4(2) FCS_CKM.4(3) FCS_COP.1(1) FCS_COP.1(2) FDP_IFC.1 FDP_IFF.1 FDP_UCT.1 FPT_ITA.1	Class FCS ensures that the TOE contains the cryptographic functionality required to meet the confidentiality aspect of the objective. Class FDP ensures that the information is only exchanged between authorised parties. FPT_ITA.1 ensures reliability of communications.
O.REPORT_STATUS_CRYPTO	FPT_ITI.1 FMT_MTD.1(1)	FPT_ITI.1 enables the TOE to detect modification of TSF data during transmission and notify the

		operator that modification has occurred. FMT_MTD.1 enables the TOE to store the operator's authorised configuration, allowing reporting if the operator is attempting to operate in a manner outside that authorisation.
O.REPORT_STATUS_SESSION	FPT_ITA.1 FPT_ITI.1	FPT_ITA.1 ensures that session setup commands and feedback are passed correctly, enabling session status reporting. FPT_ITI.1 ensures any integrity breaches during a session are detected and reported.
O.REPORT_STATUS_SYSTEM	FPT_AMT.1	FPT_AMT.1 ensures that the TOE's system status is checked at determined points and the results are provided to the operator.
O.SECRET_KEY_EXCHANGE	FCS_COP.1(1) FPT_ITC.1 FPT_ITI.1 FTP_ITC.1	FCS_COP.1(1), FPT_ITC.1 and FTP_ITC.1 extend the TOE's cryptographic operation to provide confidentiality to sensitive cryptographic information when transmitted over an insecure network. FPT_ITI.1 guards the integrity of the TSF data by monitoring for and reporting any corruption or modification.
O.SECRET_KEY_STORE	FMT_MTD.1(1) FMT_MTD.1(3) FMT_MOF.1 FMT_SMR.1	FMT_MOF.1, FMT_MTD.1(1) and FMT_MTD.1(3) restrict access to cryptographic key material to Crypto-Custodians. FMT_SMR.1 is a dependency of FMT_MTD.1
O.STORE_SECURE	FPT_PHP.3 ENV_LOCATE	ENV_LOCATE ensures that the TOE is installed in a location where it is not subject to physical attack. FPT_PHP.3 ensures that cryptographic key material is not accessible even in the event of physical access to the TOE.
OE.EDUCATE	ENV_TRAINING	ENV_TRAINING ensures that all operators are trained to operate the TOE correctly and securely.
OE.INSTALL	ENV_LOCATE ENV_INSTALL	ENV_INSTALL ensures that the Crypto-Custodian is able to configure and install the TOE correctly. ENV_LOCATE ensures that the TOE is installed in the appropriate environment.
OE.LOOK_FIRST	ENV_TRAINING	ENV_TRAINING ensures that all operators are trained to operate the TOE correctly and securely.
OE.MANAGE_KEYS	ENV_SECRETS	ENV_SECRETS ensures that sensitive cryptographic material related to the TOE is generated and handled in an appropriate manner.
OE.MANAGE_PASSWORDS	ENV_SECRETS	ENV_SECRETS ensures that security management material related to the TOE is generated and handled in an appropriate manner.
OE.TAMPER_EVIDENT	ENV_TRAINING	ENV_TRAINING ensures that an operator is able to detect evidence of an attempt to interfere with the TOE.
OE.TRAIN	ENV_TRAINING	ENV_TRAINING ensures that all operators are trained to operate the TOE correctly and securely in their authorised role(s).
OE.VET	ENV_VET	ENV_VET ensures the user organisation has

		measures in place to limit access to the TOE to trustworthy individuals.

8.2.2 Correspondence of the Security Requirements

The following table demonstrates the mappings between the security requirements (SFRs and security requirements for the non-IT environment) and the security objectives, and shows that there are no redundant elements.

Table 15. Correspondence Table for the Security Requirements

	O.ACCESS_CONTROL	O.AUTHENTICATE_RECIPIENT	O.BLACK_TRANSFER	O.COMPARTMENTALISE	O.CONFIDENTIALITY	O.REPORT_STATUS_CRYPTO	O.REPORT_STATUS_SESSION	O.REPORT_STATUS_SYSTEM	O.SECRET_KEY_EXCHANGE	O.SECRET_KEY_STORE	O.STORE_SECURE	OE.EDUCATE	OE.INSTALL	OE.LOOK_FIRST	OE.MANAGE_KEYS	OE.MANAGE_PASSWORDS	OE.TAMPER_EVIDENT	OE.TRAIN	OE.VET
FCS_CKM.1(1)					X														
FCS_CKM.1(2)					X														
FCS_CKM.2			X		X														
FCS_CKM.4(1)					X														
FCS_CKM.4(2)					X														
FCS_CKM.4(3)					X														
FCS_CKM.4(4)					X														
FCS_COP.1(1)		X			X				X										
FCS_COP.1(2)					X														
FDP_IFC.1					X														
FDP_IFF.1					X														
FDP_UCT.1					X														
FIA_UAU.1	X																		
FIA_UAU.7	X																		
FMT_MOF.1	X			X						X									
FMT_MTD.1(1)	X			X		X				X									
FMT_MTD.1(2)	X	X																	
FMT_MTD.1(3)	X									X									
FMT_MTD.1(4)	X																		
FMT_MTD.1(5)				X															
FMT_SMR.1	X									X									
FMT_SMR.3	X																		
FPT_AMT.1								X											
FPT_ITA.1					X		X												
FPT_ITC.1									X										
FPT_ITI.1						X			X										
FPT_PHP.3											X								
FTA_TSE.1		X																	

FTP_ITC.1									X									
ENV_INSTALL													X					
ENV_LOCATE											X		X					
ENV_SECRETS															X	X		
ENV_TRAINING												X		X			X	X
ENV_VET																		X

8.2.3 Dependencies and Hierarchical Relations

Dependencies and hierarchical relations obtaining within and between the SFRs are as follows:

Table 16. Dependencies and hierarchical relations within the Security Functional Requirements

Component	**Dependencies**	**Hierarchical to**
FCS_CKM.1	FCS_CKM.4 FCS_COP.1 FMT_MSA.2	-
FCS_CKM.2	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	-
FCS_CKM.4	FCS_CKM.1 FMT_MSA.2	-
FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	-
FDP_IFC.1	FDP_IFF.1	-
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	-
FDP_UCT.1	FDP_IFC.1 FTP_ITC.1	-
FIA_UAU.1	FIA_UID.1	-
FIA_UAU.7	FIA_UAU.1	-
FMT_MOF.1	FMT_SMR.1	-
FMT_MTD.1	FMT_SMR.1	-
FMT_SMR.1	FIA_UID.1	-
FMT_SMR.3	FMT_SMR.1	-
FPT_AMT.1	No dependencies	-
FPT_ITA.1	No dependencies	-
FPT_ITC.1	No dependencies	-
FPT_ITI.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FTA_TSE.1	No dependencies	-
FTP_ITC.1	No dependencies	-

Certain of the dependency relations identified above are not relevant to the TOE and have not been satisfied. The rationale for each of the unsatisfied dependencies is as follows:

Table 17. Unsatisfied dependencies

Head Component	Unsatisfied Dependency	Description and Justification
FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1	FMT_MSA.2 – Secure security attributes	This component is required to define 'secure', in terms of securely initialising security attributes. All security attributes are determined through organisation security policy so the component is not applicable.
FDP_IFF.1	FMT_MSA.3 – Static attribute initialisation	The TOE does not support creation of new objects so the component is not applicable.
FIA_UAU.1 FMT_SMR.1	FIA_UID.1 – Timing of identification	The TSF supports role-based authentication. The TSF does not support identity-based authentication. In the absence of identities, timing of identification is not applicable.

8.3 TOE Summary Specification Rationale

The TOE's security functions and assurance measures must be suitable to meet the TOE security requirements.

8.3.1 Necessity and Sufficiency of the Security Functions

The TOE's IT Security Functions identified in Section 6.1, TOE Security Functions, are necessary and sufficient to satisfy the Security Functional Requirements. Each security function is related to at least one security requirement; each requirement is required by at least one security function. The justification for the relationship in each case is shown in the table below.

Table 18. The IT Security Functions satisfy the Security Requirements

Security Functional Requirement	IT Security Function	Justification
FCS_CKM.1(1)	MK_TEK	MK_TEK performs the generation of cryptographic keys via a single ring oscillator.
FCS_CKM.1(2)	MK_UPDATE	MK_UPDATE performs the generation of cryptographic keys via a pseudo-random algorithm.
FCS_CKM.2	MK_KEK SYS_AUTH	MK_KEK enables the distribution of cryptographic key material to instances of the TOE, via the Keyfill process, which is administered within SYS_AUTH.
FCS_CKM.4(1)	MK_KEK	MK_KEK performs destruction of cryptographic keys by overwriting a previous key table with the new key table within the Keyfill process.
FCS_CKM.4(2)	MK_KEK	MK_KEK provides an emergency erase procedure to perform KEK destruction.
FCS_CKM.4(3)	MK_UPDATE	MK_UPDATE performs KEK destruction by overwriting the previous cryptographic keys each time the procedure is called or power is removed.
FCS_CKM.4(4)	MK_TEK	MK_TEK destroys cryptographic keys by overwriting the previous TEK each time a new TEK is generated, and by clearing TEK information from memory when power is removed.
FCS_COP.1(1)	F_CRY F_GOSECURE SYS_ADM SYS_AUTH	F_GOSECURE, supported by SYS_AUTH, enables the establishment of a secure communication channel, and F_CRY performs encryption and decryption of traffic exchanged across that channel. SYS_ADM permits a local user to request session establishment.
FCS_COP.1(2)	F_GOSECURE MK_TEK	MK_TEK provides random numbers from the RNG and enables IV generation. F_GOSECURE performs IV exchange as part of session establishment.
FDP_IFC.1	F_CRY	F_CRY provides encryption of the information in accordance with the traffic flow SFP.
FDP_IFF.1	F_LINE F_GOSECURE MK_KEK MK_TEK MK_UPDATE SYS_AUTH	F_LINE enables establishment of a stable communications channel, and F_GOSECURE and SYS_AUTH permit the channel to be secured. F_GOSECURE is supported by MK_KEK, MK_TEK and potentially MK_UPDATE.
FDP_UCT.1	F_CRY	F_CRY provides encryption of the information enabling their transmission in a manner protected from unauthorised disclosure.
FIA_UAU.1	F_GOSECURE SYS_AUTH	F_GOSECURE and SYS_AUTH permit activation of a secure session. SYS_AUTH controls access to and activation of KEK selection and update procedures.
FIA_UAU.7	SYS_AUTH SYS_STATUS	SYS_AUTH provides the functions involved in password access to the menu

		system. SYS_STATUS enables feedback to be provided.
FMT_MOF.1	SYS_ADM SYS_AUTH	SYS_AUTH provides the functions involved in restricting access to the menu system, which is administered under SYS_ADM.
FMT_MTD.1(1)	SYS_ADM SYS_AUTH	SYS_AUTH provides the functions involved in restricting access to the menu system, which is administered under SYS_ADM.
FMT_MTD.1(2)	SYS_ADM SYS_AUTH	SYS_AUTH provides the functions involved in restricting access to the menu system, which is administered under SYS_ADM.
FMT_MTD.1(3)	SYS_ADM SYS_AUTH	SYS_AUTH provides the functions involved in restricting access to the menu system, which is administered under SYS_ADM.
FMT_MTD.1(4)	SYS_ADM SYS_AUTH	SYS_AUTH provides the functions involved in restricting access to the menu system, which is administered under SYS_ADM.
FMT_MTD.1(5)	SYS_ADM	Access to the KEK and KEK update selection process is controlled under SYS_ADM.
FMT_SMR.1	SYS_ADM SYS_AUTH	SYS_ADM administers the roles maintained by the TSF. SYS_AUTH enables users to be identified with a role.
FMT_SMR.3	SYS_AUTH	SYS_AUTH provides the functions required to manage requests to assume authorised roles.
FPT_AMT.1	SYS_STEST SYS_STATUS	SYS_STEST enables tests to be performed to confirm the correct operation of the TOE, and SYS_STATUS permits the results of these tests to be returned to the Operator.
FPT_ITA.1	F_GOSECURE F_LINE SYS_AUTH	F_GOSECURE enables the exchange of session setup information once SYS_AUTH has confirmed the compatibility of the remote trusted IT product and a stable channel has been established under F_LINE.
FPT_ITC.1	F_GOSECURE	F_GOSECURE establishes a secure channel to enable TSF data to be transmitted securely at session setup.
FPT_ITI.1	SYS_STATUS F_LINE	F_LINE performs the functions required to detect errors in the data during transmission. SYS_STATUS provides the means of alerting this to the Operator.
FPT_PHP.3	F_TAMPER	F_TAMPER detects and reacts to attempts to gain physical access to the TOE.
FTA_TSE.1	SYS_AUTH	SYS_AUTH permits the local unit's fax authentication identifier to be compared with that requested, and authorises or denies the session accordingly.
FTP_ITC.1	F_GOSECURE	F_GOSECURE provides the functions required for the trusted channel setup data to be exchanged in an assured manner.

8.3.2 Correspondence of the Security Functions

The correspondence table below shows that each security function serves at least one security requirement, and each security requirement is served by at least one security function. The IT Security Functions and the SFRs form a consistent and mutually supporting whole.

Table 19. Correspondence Table for the Security Functions

	SYS_ADM	SYS_AUTH	SYS_STEST	SYS_STATUS	MK_KEK	MK_TEK	MK_UPDATE	F_LINE	F_GOSECURE	F_CRY	F_TAMPER
FCS_CKM.1(1)						X					

FCS_CKM.1(2)		X					X				
FCS_CKM.2		X			X						
FCS_CKM.4(1)					X						
FCS_CKM.4(2)					X						
FCS_CKM.4(3)							X				
FCS_CKM.4(4)						X					
FCS_COP.1(1)	X	X							X	X	
FCS_COP.1(2)						X			X		
FDP_IFC.1										X	
FDP_IFF.1		X			X	X	X	X	X		
FDP_UCT.1										X	
FIA_UAU.1	X	X							X		
FIA_UAU.7		X		X							
FMT_MOF.1	X	X									
FMT_MTD.1(1)	X	X									
FMT_MTD.1(2)	X	X									
FMT_MTD.1(3)	X	X									
FMT_MTD.1(4)	X	X									
FMT_MTD.1(5)	X										
FMT_SMR.1	X	X									
FMT_SMR.3		X									
FPT_AMT.1			X	X							
FPT_ITA.1		X						X	X		
FPT_ITC.1									X		
FPT_ITI.1				X				X			
FPT_PHP.3											X
FTA_TSE.1		X									
FTP_ITC.1									X		

8.3.3 Necessity and Sufficiency of the Assurance Measures

The assurance measures identified in Section 6.2, Assurance Measures, are necessary and sufficient to satisfy the Security Assurance Requirements. Each assurance measure is required to meet at least one assurance requirement; each requirement is met by at least one assurance measure. The justification for the relationship in each case is shown in the table below.

Table 20. The Assurance Measures satisfy the Assurance Requirements

Assurance Requirement	Assurance Measure	Justification
ACM_CAP.1	Configuration Management	ACM_CAP.1 requires the TOE to be labelled with a reference unique to its version. CES03/32 enables tracking of version numbers for the engineering, documentation and support elements involved in maintaining the TOE.
ADO_DEL.1	Safe Delivery Procedure	ADO_DEL.1 requires procedures to be documented and followed which shall ensure security of the TOE in transit to a user organisation. CES03/40 and CES03/42 document the steps required prior to shipment to allow interference with the shipment to be detected. CES03/41 and the SQ-Phoenix

		Installation and Start-Up Guide document the steps required upon receipt to detect such interference.
ADO_IGS.1	Safe Configuration and Installation Directions	The SQ-Phoenix Operating Manual and SQ-Phoenix Installation and Start-Up Guide document the procedures required to securely install the TOE and prepare it for operation.
ADV_FSP.1	Development Documentation	CES03/33 describes the external interfaces of the TSF, and the purposes, uses and feedback supplied by these.
ADV_HLD.1	Development Documentation	CES03/34 describes the structure of the TSF in terms of subsystems and the security functionality provided by each of these. The document further identifies and describes interfaces to the subsystems, and overviews the TSF's hardware, software and firmware.
ADV_RCR.1	Development Documentation	CES03/33 relates the external interfaces of the TSF to the security functions outlined in CES03/31. CES03/34 relates the TSF's subsystems to the interfaces described in CES03/33.
AGD_ADM.1	User Guidance	The SQ-Phoenix Operating Manual and SQ-Phoenix Installation and Start-Up Guide contain administrative guidance describing the TOE's functions and interfaces and how to administer the TOE securely, including privileges which may need to be restricted.
AGD_USR.1	User Guidance	The SQ-Phoenix User Guide describes the functions and interfaces available to TOE Operators and instructs Operators on the behaviour required to maintain the TSF.
ATE_COV.1	Test Procedures Development Documentation	ATE_COV.1 requires a correspondence to be drawn between the tests outlined in the test documentation and the TSF. The TSF is described in CES03/33, CES03/19 comprises the test documentation, and CES03/36 relates the testing to the TSF.
ATE_FUN.1	Test Procedures	CES03/19 describes the procedures undertaken in testing the TSF and the results achieved. CES03/36 describes the goals of each test set. CES03/10 places the test process in context in the TOE's development management and facilitates interpretation of the results compared to expectations.
ATE_IND.2	Test Procedures	The developer has supplied the evaluator with resources equivalent to those used in the functional testing to permit a sample of the functional tests to be conducted.
AVA_SOF.1	Vulnerability Assessment	CES03/35 calculates the strength of TOE security functions identified in the ST as having a strength of TOE security function claim.
AVA_VLA.1	Vulnerability Assessment	CES03/35 reviews the TOE deliverables for obvious vulnerabilities which could be exploited to violate the TSP.

8.3.4 Correspondence of the Assurance Measures

The correspondence table below shows that each assurance requirement is met by at least one assurance measure, and each assurance measure is required by at least one assurance requirement.

Table 21. Correspondence Table for the Assurance Requirements

	ACM_CAP.1	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
Configuration Management	X												
Safe Delivery Procedure		X											
Safe Configuration and Installation Directions			X										
Development Documentation				X	X	X			X			X	X
User Guidance							X	X					
Test Procedures									X	X	X		
Vulnerability Assessment												X	X

8.3.5 Suitability of the Assurance Requirements

The TOE is designed to meet an evaluation assurance level of EAL2, and the assurance requirements are consistent with this. EAL2 is consistent with the minimum level required for protection of information not of national security importance and unclassified but restricted to the level of PROTECTED or HIGHLY PROTECTED.

8.3.6 Strength of Function Rationale

The TOE is claimed to have an overall strength of function SOF-basic. This claim is justified in view of the minimum strength of function claimed in subclauses of Section 6.1, TOE Security Functions, and is consistent with the targeted evaluation assurance level EAL2.

8.4 PP Claims Rationale

No claims are made of conformance with any PP.