Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 35/2005

April 2005

Version 1.0

Amendment Record

Version	Date	Description
1.0	April 2005	Public release.

Executive Summary

1 The SQ-Phoenix Digital Encryptor Version 2.7 is an in-line encryptor for voice and fax communications over analogue transmission networks. It is designed to protect the confidentiality of sensitive information during transmission. SQ-Phoenix Digital Encryptor Version 2.7 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of CES Communications Ltd's SQ-Phoenix Digital Encryptor Version 2.7, to the Common Criteria (CC) evaluation assurance level EAL 2. The report concludes that the product has met the target assurance level of EAL 2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by Tenix Defence AISEF and was completed in March 2005.

3 The Australasian Certification Authority (ACA) recommends that users:

a) Set up the TOE for use in its evaluated configuration.

b) Verify that AES is installed on each SQ-Phoenix unit by establishing a *Secure Voice* call to another SQ-Phoenix unit which is known to have AES installed.

c) Implement a suitably secure key exchange infrastructure.

4 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

5 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

6 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, SQ-Phoenix Digital Encryptor Version 2.7, against the requirements of the Common Criteria (CC) evaluation assurance level two (EAL 2); and

b) provide a source of detailed security information about the TOE for any interested parties.

7 This report should be read in conjunction with the TOE's Security Target (Ref [1]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

8 Table 1, provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	SQ-Phoenix Digital Encryptor Version 2.7
Software Version	N/A
Security Target	Security Target Version 1.3, March 2004 for SQ-Phoenix Digital Encryptor Version 2.7
Evaluation Level	EAL 2
Evaluation Technical Report	Evaluation Technical Report for SQ-Phoenix Digital Encryptor 2.7, March 2005
Criteria	CC Version 2.1, August 1999, with interpretations as of 14 August 2003
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 14 August 2003
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	CES Communications Ltd
Evaluation Facility	Tenix Defence AISEF

Table 1 - Identification Information

Chapter 2 - Target of Evaluation

2.1 Overview

9 This chapter contains information about the Target of Evaluation (TOE) including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

10 The TOE is the SQ-Phoenix Digital Encryptor Version 2.7 developed by CES Communications Ltd. Its primary role is to protect the confidentiality of sensitive voice and fax information during transmission over analogue networks.

11 The SQ-Phoenix takes data from the operator's communications equipment, digitises it if necessary, and encrypts it for transmission across the communications network. Digital transmission across the analogue network is accomplished using the V32.bis modem protocol and commercial communications components.

12 The SQ-Phoenix is administered and managed by authenticated users. Any individual with physical access to the SQ-Phoenix can operate it and choose whether to invoke the product's security functions. In the evaluated configuration, encryption is performed using the AES 128 digital encryption algorithm and 128-bit keys. The evaluated configuration is a subset of the SQ-Phoenix's total functionality.

13 The SQ-Phoenix provides single-session operation and cannot be used for multiple concurrent secure communication sessions, even by the same operator. In addition, the product has been designed for deployment in a wide variety of telecommunications situations and has selectable settings for operation in different environments.

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. Although the Security Target (Ref [1]) contains no explicit security policy statements, the following TOE Security Policies (TSPs) are implied:

- Confidentiality of sensitive cryptographic material stored within the SQ-Phoenix.

- Confidentiality of sensitive information in transmission across an un-trusted channel.

- Integrity of sensitive information in transmission across an un-trusted channel.

- Authentication of the intended recipient of a secure fax transmission.

15 These elements of the security policy are described within the SQ-Phoenix as a collection of security services as defined in Table 2. The services are realised as the security functions requirements of the TOE.

Security Service	**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
Communication 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

Table 2 - Security Services

2.4 TOE Architecture

16 The TOE consists of the following major architectural components:

a) Hardware:

i) **Main Board**: provides the power, the external interfaces and the microprocessors of the TOE. The microprocessors are the Atmel AVR microcontrollers and the Programmed Logic Device (PLD). The anti-tamper and emergency erase functions are also hosted on the main board.

ii) **Options Board**: contains the core cryptographic processing unit, the SQ-Phoenix Cryptographic Processor (SQCP), and its supporting EEPROM and RAM.

iii) **Keyboard Assembly**: contains the user interface LCD and keypad which is interfaced to the main board via a ribbon cable.

b) Software:

i) **AVR firmware**: is the main processing firmware and provides the controlling monitor for the TOE. This includes the various device drivers for interfacing to and driving the user peripherals, the menu and configuration subsystems, and the interface to the SQCP.

ii) **SQCP firmware** controls the cryptographic functions of the TOE.

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

- **Cryptographic Support:** Cryptographic operations are implemented to support data encryption/decryption, digital signature verification, key agreement and hashing. The TOE performs encryption using the AES 128 algorithm. Externally generated key encrypting keys (KEKs) are used to encrypt the session unique traffic exchange keys (TEKs) during key exchange. Multiple cryptographic keys are supported to allow compartmentalisation.

- **User Data Protection:** The TSF enforces access control to objects based on the operator's desire to transmit information securely.

- **Identification and Authentication:** The TSF allows secure session requests, key exchange updates and key exchange key selection. Access to the Administrator and Crypto-Custodian roles is by a password. The TOE can be requested to authenticate the recipient in a secure fax transmission to prevent accidental transmission of sensitive information to an unauthorised recipient.

- **Security Management:** The ability to query, modify or load crypto configuration information, crypto keys, crypto algorithms, cipher chain settings and the default net are restricted to the Crypto-Custodian. The ability to modify the Crypto-Custodian and Administrator passwords is restricted to the Crypto-Custodian and Administrator respectively. Finally, the ability to modify the selected KEK number and KEK update cycle number is restricted to the operator.

- **Protection of the TSF:** The TSF runs a self-diagnosis during initial start-up to demonstrate its correct operation. In addition it protects data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure with notifications of attempted modifications. Finally, the TOE provides the operator the ability to zeroise sensitive cryptographic material via a switch on the rear of the unit. The TOE will automatically invoke the zeroise function if the unit is opened.

2.5.2 Non-evaluated Functionality

19 Potential users of the TOE are advised that a set of functions and services has not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government ICT Security Manual (ACSI 33) (Ref [2]) for guidance on this matter. New Zealand Government users should consult the GCSB. The functions and services that have not been included as part of the evaluation are provided below:

a) All key management configurations other than *Net Mode*.

b) Encryption using cryptographic algorithms other than AES 128.

c) Cipher chaining in electronic codebook mode (ECB).

d) Operation without dedicated cryptographic circuitry.

e) Secure file transfers over the secure voice link.

f) Ancillary support equipment.

2.6 Usage

2.6.1 Evaluated Configuration

20 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to ACSI 33 (Ref [2]) for Australian Government policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the GCSB.

21 The TOE is configured before deployment to use AES 128 algorithm in Cipher Feedback (CFB) mode with 128-bit keys. The evaluated configuration uses a key management configuration termed *Net Mode.* In this configuration the TOE is electronically loaded with externally generated 128-bit key exchange keys (KEK). One-time 128-bit traffic exchange keys (TEKs) are generated internally at the start of each secure session.

2.6.2 Delivery procedures

22 When placing an order for the TOE, purchasers should make it clear to Signal Guard, the company that markets and sells the TOE, that they wish

to receive the evaluated product. They should then receive a facsimile containing the:

a) Packing slip containing the serial numbers of the units to be delivered.

b) SG03/41 SQ-Phoenix Delivery Acceptance Procedure (Ref [3]).

23 Signal Guard will telephone to confirm that the information has been received and that the originals will be placed with the packing documentation.

2.6.3 Determining the Evaluated Configuration

24 The Delivery Acceptance Procedure (Ref [3]) provided to the purchaser both prior to delivery and in the packing material advises:

a) To check that the serial numbers match the serial numbers that were provided by Signal Guard in the original facsimile.

b) To ensure that the six screws are in place in the bottom of the unit and that the tamper-evident seals are intact.

c) If the customer suspects the units have been tampered with, modified or otherwise interfered with during delivery they should contact Signal Guard immediately. Signal Guard will then take appropriate action.

25 The received TOE will have been set to factory default values for all configuration items. The guidance on installing the product in its evaluated configuration is contained in the Installation and Startup documentation (Ref [4]) and the Operating Manual (Ref [5]). These procedures will result in a secure configuration that is consistent with the evaluated configuration defined in the Security Target.

2.6.4 Documentation

26 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided with the TOE:

a) SG03/41: SQ-Phoenix Delivery Acceptance Procedure, v1.1, 3 March 2004, 030304-110 (Ref [3])

b) SG03/I: SQ-Phoenix Installation and Startup, v1.2, 4 March 2004, 040304-120 (Ref [4])

c) SG03/O: SQ-Phoenix Digital Encryptor Operating Manual, v2.72, 4 March 2004, 040304-272 (Ref [5])

2.6.5 Secure Usage

27 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

a) Administrators and Crypto-Custodians are non-hostile and follow all administrator guidance and abide by all organisational security policies.

b) 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.

c) The operator will choose whether or not to invoke the security functions available from the TOE.

d) Operators may not be equally privileged or have access to all sensitive information. The TOE will be configured to reflect its operator's access privileges.

e) The product incorporates measures to ensure that electromagnetic radiation does not allow cryptographic variables or sensitive information to be transmitted without protection into the insecure environment.

f) 128-bit KEKs are generated externally to 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.

g) The TOE will be operated in a controlled environment which has been secured in accordance with the guidance in the SQ-Phoenix Installation and Startup Guide (Ref [4]). All individuals with authorised physical access to the installed location are assumed to be authorised to operate the TOE.

h) 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).

28 In addition, the following organisational security policy statements must be in place:

a) 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.

b) Technical and physical assurance procedures will be defined and rigorously enforced for generation, distribution, change and handling of all cryptographically relevant material.

c) 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).

Chapter 3 - Evaluation

3.1 Overview

29 This chapter contains information about the procedures used in conducting the evaluation, and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

30 The criteria against which the TOE has been evaluated are expressed in the Common Criteria for Information Technology Security Evaluation (Refs [6], [7], [8]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [9]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [10], [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA) (Ref [12]) were also upheld.

3.3 Functional Testing

31 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

32 The functional testing effort also included a selection of independent functional tests. The independent tests principally exercised each TSF with a strength of function claim as well as those TSF that were not included in the developers original tests.

3.4 Penetration Testing

33 The developer performed a vulnerability analysis of the SQ Phoenix in order to identify any obvious vulnerability in the product and to show that the vulnerability is not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information such as documentation concerning the

AES 128 algorithm, and an Atmel engineering data book for the AVR microcontroller. The developer identified a number of potential vulnerabilities and in each case was able to show that the vulnerability was not exploitable in the TOE's intended operational environment.

34 Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test plan. After the completion of testing, the evaluators were able to determine that the TOE, in its intended configuration and environment, has no obvious exploitable vulnerabilities.

Chapter 4 - Certification

4.1 Overview

35 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

36 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of SQ-Phoenix Digital Encryptor Version 2.7 performed by the Australasian Information Security Evaluation Facility, Tenix Defence AISEF.

37 Tenix Defence AISEF has found that SQ-Phoenix Digital Encryptor Version 2.7 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level two, EAL 2.

38 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

39 EAL 2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

40 The analysis is supported by: independent testing of the TOE security functions; evidence of developer testing based on the functional specification; selective independent confirmation of the developer test results; strength of function analysis; and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

41 EAL 2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.4 Recommendations

4.4.1 Cryptography

42 The evaluation of the cryptographic functions of the SQ-Phoenix is beyond the scope of the Common Criteria evaluation and has been undertaken as a separate process by the Defence Signals Directorate, the national cryptographic authority for Australia. The AES 128-bit encryption algorithm as implemented by the SQ-Phoenix has been tested and verified in the CFB mode of operation. The key generation and

exchange infrastructure has also been tested and verified. It is recommended that users:

a) Verify that AES is installed on each SQ-Phoenix unit by establishing a *Secure Voice* call to another SQ-Phoenix unit which is known to have AES installed.

b) Implement a suitably secure key exchange infrastructure.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for SQ-Phoenix Digital Encryptor Version 2.7. Version 1.3, March 2004

[2] Australian Communications Security Instruction 33 (ACSI 33), Australian Government Information and Communications Technology Security Manual, Defence Signals Directorate, (available at www.dsd.gov.au)

[3] SG03/41: SQ-Phoenix Delivery Acceptance Procedure, v1.1, 3 March 2004, 030304-110

[4] SG03/I: SQ-Phoenix Installation and Startup, v1.2, 4 March 2004, 040304-120

[5] SG03/O: SQ-Phoenix Digital Encryptor Operating Manual, v2.72, 4 March 2004, 040304-272

[6] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-08-14

[7] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 2003-08-14

[8] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 2003-08-14

[9] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2003-08-14

[10] AISEP Publication No. 1 – Description of the AISEP, AP 1, Version 2.0, February 2001, Defence Signals Directorate

[11] AISEP Publication No. 2 – The Licensing of the AISEFs, AP 2, Version 2.1, February 2001, Defence Signals Directorate.

[12] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[13] EFTT001D0044 Evaluation Technical Report for SQ-Phoenix Digital Encryptor 2.7, Issue 3.0

A.2 Abbreviations

ACA	Australasian Certification Authority
AES 128	Advanced Encryption Standard 128-bit
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
AVR	Atmel AVR microcontroller
CC	Common Criteria
CFB	Cipher Feedback Mode
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ECB	Electronic Codebook Mode
EEPROM	Electronically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
KEK	Key Exchange Key
LCD	Liquid Crystal Display
PLD	Programmed Logic Device
PP	Protection Profile
RAM	Random Access Memory
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
SQ-Phoenix	SQ-Phoenix Digital Encryptor Version 2.7
SQCP	SQ-Phoenix Cryptographic Processor
TEK	Traffic Exchange Key
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy