UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

CERTIFICATION REPORT No. P160

SureWare Keyper Professional

Version 2 Release 1

Issue 1.0

October 2001

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

RECOGNITION AGREEMENT OF
INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Agreement Group and as such:

- indicates that it is the issuer's claim that this certificate is a conformant certificate as defined in this Agreement; and

- therefore gives grounds for confidence, though it cannot in itself guarantee, that the certificate is a conformant certificate and that it will in practice be recognised by the other Members of the Agreement Group.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

CERTIFICATION STATEMENT

Baltimore's SureWare Keyper Professional is a dedicated embedded computer, which provides cryptographic services (key generation, signing, MACing) for applications on host computer systems.

SureWare Keyper Professional, Version 2 Release 1, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the requirements of ITSEC Assurance Level E3 for the mechanisms that protect these services.

Originator	**CESG** Certifier
Approval	**CESG** Deputy Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	22 October 2001

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

API	Application Programming Interface
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CSE	Canadian Security Establishment
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSD	Defence Signals Directorate
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HMG	Her Majesty's Government
HSP	Hardware Security Processor
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKCS#11	Public Key Cryptography Standard Number 11
RNG	Random Number Generation
RSA	Rivest, Shamir and Adleman. (An asymmetric cryptographic algorithm suitable for both encryption and digital signatures.)
RTC	Real Time Clock
SCM	Software Configuration Management
SEF	Security Enforcing Function
SHA-1	Secure Hash Algorithm as defined in FIPS 180-1
SIN	Scheme Information Notice
SMK	Storage Master Key
SoM	Strength of Mechanisms
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, 2 February 2000.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. SureWare Keyper Professional, 010387 ITSEC Security Target,
Baltimore Technologies Limited,
Version 3.3, 2 August 2001.

d. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

e. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

f. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

g. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

h. ITSEC Joint Interpretation Library (ITSEC JIL),
Joint Interpretation Working Group,
Version 2.0, November 1998.

i. LFF/T217 Evaluation Technical Report,
IBM Global Services CLEF,
LFF/T217/ETR,
Issue 1.1, 6 August 2001.

j. FIPS PUB 140-1, Security Requirements for Cryptographic Modules,
National Institute of Standards and Technology,
11 January 1994.

k. PKCS#11, Cryptographic Token Interface Standard,
RSA Laboratories,
Version 2.01, December 1997.

l. Baltimore SureWare Keyper Professional User Guide,
Baltimore Technologies Limited,
COM010578, Version 2.2, 6 June 2001.

m. Storage, Handling and Transit of Secure Product,
Baltimore Technologies Limited,
9002-M1, Version 0.2, 22 February 2000.

n. FIPS 140-1, Certificate 146,
23 April 2001.

I. INTRODUCTION

Intended Audience

1. This Certification Report states the outcome of the IT security evaluation of SureWare Keyper Professional Version 2 Release 1 to the Sponsor, Baltimore Technologies Ltd., and is intended to assist potential users when judging the suitability of the product for their particular requirements.

Identification of Target of Evaluation

2. The version of the product evaluated was:

SureWare Keyper Professional Version 2 Release 1.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Baltimore Technologies Ltd.

3. Baltimore's SureWare Keyper Professional is a cryptographic provider which connects to a host computer via standard networking technology in order to provide secure cryptographic services to host computer applications: key generation, Message Authentication Code, (MACing), signing. These applications will communicate with the SureWare Keyper Professional via the industry standard interface, PKCS#11, [Reference k].

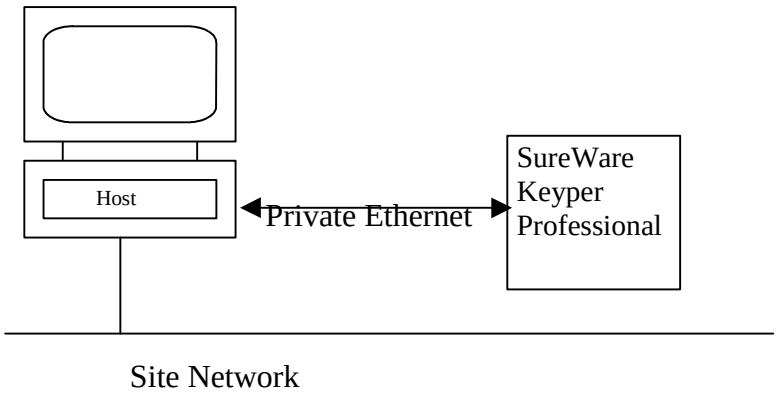

Figure 1 - TOE Connections

Scope of Evaluation

3. The TOE boundary was the physical enclosure of SureWare Keyper Professional: the scope of the evaluation did not include either the connected host computer or any of its applications; it also did not include the tamper resistant properties of the physical enclosure (but see paragraph 9).

4. The scope of the evaluation covered those mechanisms that protect the cryptographic services that the TOE provides. The cryptographic mechanisms, Triple DES, RSA, DSA and SHA-1 contained within the TOE are publicly known.

Evaluation

5. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme, as described in UKSP 01 and UKSP 02 [a, b]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty's Government.

6. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [c], which prospective users are advised to read. (A copy of the Security Target may be obtained from Baltimore Technologies Ltd.) The criteria against which the TOE was judged are described in the IT Security Evaluation Criteria (ITSEC) [d]. This describes how the degree of assurance is expressed in terms of the levels E0 to E6 where E0 represents no assurance. The methodology used is described in the IT Security Evaluation Manual (ITSEM) [e], UKSP 05 [f, g] and the ITSEC Joint Interpretation Library [h].

7. The Certification Body monitored the evaluation, which was carried out by the IBM Global Services Commercial Evaluation Facility (CLEF). The evaluation was completed in August 2001, when the CLEF submitted an Evaluation Technical Report (ETR) [i] to the Certification Body, which formed the basis of this Certification Report.

8. The Target Assurance Level for the product, as required by the Security Target [c], was E3.

9. The implementation of Triple DES, DSA and SHA-1 has been validated under the NIST/CSE Cryptographic Evaluation Scheme as certified by FIPS 140-1 Certificate 146 [n]. This FIPS Certificate also covered SureWare Keyper Professional's Random Number Generation (RNG) and tamper resistance properties. Furthermore, CESG assessed SureWare Keyper Professional's tamper resistance enclosure. Baltimore supplied test results comparing a third party independently implemented software implementation of RSA with SureWare Keyper Professional's hardware implementation. As the two implementations of RSA produced identical test results against different multiple precision libraries, the Certifier was satisfied that RSA within SureWare Keyper Professional was correctly implemented. The Certifier witnessed Baltimore's RSA testing. Additionally, DSD confirmed the correctness of SureWare Keyper Professional's implementation of RSA.

10. SureWare Keyper Professional is not currently approved to handle HMG protectively marked data.

General Points

11. Prospective users of the TOE are reminded that the security functionality evaluated is that claimed in the Security Target [c]. This functionality may not necessarily meet all the threats that a user has identified in a particular operating environment. The assumed threats, intended method of use and environment are as stated in the Security Target. The TOE should only be used in its evaluated configuration (as indicated in Annex B) and in accordance with the recommendations and caveats contained in this report. It is the responsibility of purchasers to ensure that SureWare Keyper Professional Version 2 Release 1 meets their requirements.

12. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Users (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been evaluated and certified.

13. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

14. The evaluation of SureWare Keyper Professional Version 2 Release 1 followed the generic Evaluation Work Programme described in the ITSEM [e], with work packages structured around the evaluator actions described in the ITSEC [d]. The results of this work were reported in the ETR [i] under the ITSEC headings. This Certification Report summarizes the assurance results in relation to the security functionality claimed in the Security Target [c].

Correctness - Construction

15. This aspect of the evaluation examined both the development process (i.e. the Security Target, the Architectural and Detailed Designs, the Implementation) and the environment in which it took place. The results were as follows:

a. The final version of the Security Target [c] described the Security Enforcing Functions (SEFs) provided by the TOE, and contained a product rationale identifying its method of use, intended environment and relevant threats; it also described how the product's functionality was appropriate for that method of use and was adequate to counter the assumed threats.

b. The Architectural Design provided an adequate description of the general structure of the TOE, together with any external interfaces, referring out to the hardware description documentation for a more detailed description of hardware. Although not explicitly described, it was possible to identify the separation between security enforcing and other components.

c. The Detailed Design documentation was supplied in the form of a Rational Rose model and a document mapping basic components to the source code. The documentation described the realization of all security enforcing and security relevant functions. All security mechanisms were identified, and their specifications and definitions provided. The Rational Rose model showed how each security mechanism was implemented and their relationship with each component.

d. All SEFs were correctly implemented in Version 2 Release 1 of the source code. The Developer supplied five documents to meet the requirement for the testing of the TOE. These documents contained descriptions of the set-ups used for testing, a test plan and descriptions of the purpose of the tests. All tests and results of testing were uniquely numbered. The test descriptions were sufficient to ensure that the tests were repeatable, and the tests were adequate for testing the SEFs. The test results were documented in the form of a test report. All the tests were recorded as having a pass verdict assigned to them. Test documentation showed that re-testing following the correction of errors was carried out, and this was confirmed during the Development Environment Assessment visit. The test documentation covered all the SEFs and mechanisms identified in the Detailed Design and source code. The tests were adequate for exercising the security functionality at these levels.

e. The configuration control, programming standards and security aspects of the Developer's working environment were satisfactory.

f. The configuration control system in use for the SureWare Keyper Professional is the Perforce Software Configuration Management (SCM) tool, which is fully documented. In addition to the configuration control of the software components, Perforce SCM is used to store and control relevant hardware drawings and design information together with software design documentation, test plans and product manuals etc. During the development environment inspection visit, the Evaluators were able to confirm that the documented procedures were being followed. The programming language used for development is C++, which has an agreed and well defined syntax. A suite of software (WindRiver Systems DiabData 4.3f) was used to compile C++ source code.

g. The TOE hardware is assembled on a sub-contractor's HMG security accredited premises. Security procedures ensured the integrity of the TOE and the confidentiality of the associated documentation. The security procedures were based on proven information security principles and no errors were identified. A check that the documented procedures were being applied was performed during the Development Environment Assessment. No errors or omissions were discovered in the documented security measures.

16. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of its Security Target, Architectural and Detailed Designs, Implementation and Development Environment.

Correctness - Operation

17. The Evaluators checked and confirmed that:

a. The operational documentation adequately described the SEFs relevant to users and how to operate the TOE in a secure manner. Guidelines for Administrators are detailed in the User Guide [l] and describe the precautions which are to be taken to avoid compromising the confidentiality of the data transmitted. Protection against theft and unauthorised use is specified. On power up, a Security Officer must authorise SureWare Keyper Professional's use as a provider of cryptographic services, and whilst not in use, the Security Officer can authorise the SureWare Keyper Professional to withdraw cryptographic services. The guidelines also provide details of initialisation, single/multi-unit sites, upgrading from HSP 4000, network set-up, key management and the return to factory procedure.

b. The delivery and configuration documentation [m] described the delivery arrangements from the development environment to the customer and the required system generation aspects. The TOE is dispatched in a sealed tamper-evident bag with the tamper bag serial number being sent independently to the customer. The TOE is transported by an approved courier with the keys being sent separately via

registered post. Configuration options are described, along with a description of their impact on the security of the TOE.

c. The procedures for startup and operation are described in the User Guide [l]. As part of the penetration testing, the Evaluators repeated the startup procedure using only the instructions provided in user documentation.

18. The Evaluators concluded that the Operational Documentation and the Operational Environment met the requirements for ITSEC E3.

Effectiveness - Construction

19. This aspect of the evaluation dealt with:

a. The suitability of the TOE's SEFs to counter the threats identified in the Security Target [c].

b. The ability of the SEFs and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole.

c. The ability of the TOE's security mechanisms to withstand direct attack.

d. The question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

20. The Evaluators were satisfied that:

a. The Suitability Analysis confirmed that all the threats listed in the Security Target [c] were adequately countered by one or more of the stated SEFs and mechanisms. The SEFs were correlated to the intended method of use and the intended environment for the product. Also included were the dependencies on non-IT security measures assumed to be provided by the environment. Finally, the assumptions about the environment into which the TOE was to be installed were provided.

b. The Binding Analysis demonstrated that it was not possible for any SEF or mechanism to conflict with or contradict the intent of any other SEF or mechanism. The Binding Analysis listed all ways in which the SEFs and security mechanisms could interact. It showed that none of the SEFs could conflict with or contradict the intent of another SEF or mechanism.

c. The countermeasures proposed by the Sponsor in the List of Known Vulnerabilities in Operational Use were entirely satisfactory.

d. The Strength of Mechanisms (SoM) Analysis listed all the security enforcing mechanisms identified as critical within the TOE; six of the security mechanisms fell in the category of cryptographic strength of mechanism; six security mechanisms were non-critical.

21. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Suitability, Binding, SoM and Construction Vulnerability.

Effectiveness - Operation

22. This work involved:

a. Checking that the TOE can be used in a secure manner and assessing whether known vulnerabilities in its operation could, in practice, compromise its security; and

b. Checking the List of Known Vulnerabilities in the operation of the TOE, as supplied by the Sponsor, and assessing the impact of these vulnerabilities and the measures proposed to counter their effects.

23. The evaluation confirmed that:

a. Any error in operation of the TOE would not result in the disabling of any SEFs or security mechanisms. Also, it is not possible to configure the TOE in a way that would allow it to be used in an insecure way. The Ease of Use Analysis identified six possible modes of operation of the TOE, including details concerning operation following failure, operational error and their consequences and implications for maintaining secure operation. The six modes of operation are:

i. Initialised state
ii. Operational state
iii. Operational Tamper state
iv. Shutdown mode
v. Download state
vi. Management state.

b. Penetration testing confirmed that none of the known vulnerabilities are actually exploitable in practice.

24. The Evaluators concluded that the TOE met the requirements for ITSEC E3 in respect of Ease of Use and Operational Vulnerability.

Specific Functionality

25. The Evaluators concluded that all the functionality claimed in the Security Target [c] had been met. Security functionality ensures that data leaving the TOE's external interfaces is in enciphered form and that cryptographic keys are suitably generated and used only for their intended purpose.

26. Three categories of key (all of which are used in Triple DES encipherment) exist within the TOE's key hierarchy:

- Authorization Key. This protects the TOE from unauthorized access by providing a means to authenticate Security Officer smartcards.

- Storage Master Key (SMK). This is used to wrap the application keys.
- Application Key. Application keys are generated by a request for cryptographic services, i.e. a key generation request by a host.

27. Key material is contained in a tamper-resistant enclosure. In keeping with paragraph 1.3 of ITSEC [d], it should be noted that tamper resistant properties were not covered by the E3 evaluation. For information on tamper resistance assurance, the reader is referred to [n].

28. In the event of tamper being detected, all keys are erased. Two types of tamper are catered for:

a. Positive tamper, which requires that the TOE be returned to the manufacturer for operational re-enablement; and

b. Operational tamper, which means that the TOE can be recovered by clearing the tamper condition, using the TOE keypad menu and re-importing the SMK and application keys from smartcard.

(This page is intentionally left blank)

III. CONCLUSIONS

Certification Result

29. After due consideration of the ETR [i], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that SureWare Keyper Professional Version 2 Release 1 meets the requirements of ITSEC Assurance Level E3 for the mechanisms that protect the cryptographic services.

Recommendations

30. SureWare Keyper Professional should only be used in accordance with the intended environment and method of use described in the Security Target [c]. Particular care should be taken that it is used in accordance with operational documentation [l, m].

31. Potential users of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [c].

32. It is recommended that Baltimore Technologies include guidance to administrators on connecting a terminal, PC or PDA to the serial port during installation in order to view any errors.

33. Concerning the protection of user data against modification, software on the host computer used to verify and warn the user of possible modification was not within the scope of evaluation. It is therefore assumed that the application verifying data on the host machine will report any possible tamper.

(This page is intentionally left blank)

ANNEX A: SUMMARY OF THE SECURITY TARGET

Introduction

1. The Security Target is given in [c]. The Product Rationale is summarised below.

Product Rationale

Intended Method of Use

2. The SureWare Keyper Professional is a small desktop unit, comprising a dedicated, embedded computer, which provides applications on host machines with cryptographic services. The host machine communicates with SureWare Keyper Professional via standard networking technology and via a standard software interface – PKCS#11 [k].

3. In addition to an ethernet interface, SureWare Keyper Professional provides interfaces for import/export of cryptographic keys via tokens and has a small keypad for input of configuration data and/or input of PINs where required.

Assumed Threats

General

4. Malfunction of the TOE (e.g. software fault, processor, Real Time Clock (RTC), RNG, tamper circuitry, program memory, data memory) reveals key material or sensitive data and/or prevent use of TOE functions.

5. Leakage of key material, sensitive message data or weakening of the crypto algorithm caused by malformed API calls or use of non-API routines to access the TOE.

6. Alteration of the TOE's RTC.

Crypto

7. Unintentional modification of security sensitive data or key material.

8. Random numbers used as key seeds are not truly random.

9. Recording of sensitive keys before and after cryptographic functions.

10. Unauthorised access to confidential data.

Physical

11. Tampering Electrically (varying power supply, injecting noise, injecting signals on network connections), mechanically (drilling holes to inspect or attach probes) or utilising temperature changes to gain access to key material or sensitive message data.

12. Modification of a component of the TOE.

13. Replacement of the TOE with a Trojan Horse.

Digital Signature Threats

14. A user may attempt to sign data with the private key of another user, thus impersonating him.

15. The digital signatures may not offer a sufficiently high degree of protection against modification.

16. An attacker could gain possession of both the encrypted private key and all components of the key (SMK) used to protect it. Hence the attacker could obtain and employ the values of the keys in other equipment.

Summary of Security Features

17. Keys generated by the SureWare Keyper Professional utilise a pseudo-random sequence which is frequently re-seeded from a hardware noise source.

18. Where keys are generated for use with digital signatures, the pseudo-random sequence is suitably random – i.e. a "FIPS approved" generator based on publicly known cryptographic techniques (i.e. SHA-1) is employed.

19. The TOE provides no software functionality which present any plain text private or secret keys to any external interface.

20. Private or secret Administrator keys presented to the SmartCard interface are in component form. (The export of private administration keys is restricted to component form only.)

21. Administrators can prevent the export of the internal SMK. This can normally be exported in component form, but a configuration option is provided to permanently prevent this. (This feature was implemented in Version 2, Release 1 to comply with German digital signature legislation.)

22. Keys can only be used for the purposes for which generated.

23. The TOE zeroises cryptographically sensitive data (plaintext keys) if its physical environment is compromised. (See [n].)

24. Administrators are authenticated before being able to undertake administrative actions.

25. User provided data is protected against undetectable modification and/or authenticated as originating from a particular entity via digital signatures (where users request this service) employing publicly known techniques (either RSA or DSA by user option).

26. Although not a Security Enforcing Function in the ITSEC sense, the TOE also implements a tamper detecting and response mechanism which conforms to the requirements of FIPS PUB 140-1 at level 4 [j].

Target Assurance Level

27. The Target Assurance Level for the product, as defined in the Security Target [c], was E3 as defined in ITSEC [d].

(This page is intentionally left blank)

ANNEX B: EVALUATED CONFIGURATION

Firmware

1. The following firmware was installed on the TOE:

    a. Application Boot Loader, Version 9, Revision 4;

    b. Loader, Version 3, Revision 3; and

    c. Host Security Module Server, Version 2, Revision 7.

Note: All software is embedded in firmware for the operational TOE.

Hardware

2. SureWare Keyper Professional, Baltimore part number 9620, Version 2, Release 1.

(This page is intentionally left blank)