Certification Report

EAL 4+ (ALC_FLR.2)
Evaluation of

TÜBİTAK BİLGEM UEKAE

KERMEN PORTABLE v1.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	04.09.2013
Version of Report	1.0
Author	Murat ADSIZ
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	04.09.2013
Certification Report Number	21.0.01/13-028
Sponsor and Developer	TÜBİTAK BILGEM UEKAE
Evaluation Lab	TÜBİTAK BILGEM OKTEM
TOE/ PP Name*	Kermen Portable v1.0
Pages	15

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
v1.0	04.09.2013	All	First released

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Committee the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Testing Laboratory (CCTL) under CCCS' supervision.

CCTL is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BILGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Kermen Portable v1.0 whose evaluation was completed on 03.09.2013 and whose evaluation technical report was drawn up by TÜBİTAK BILGEM OKTEM (as CCTL), and with the Security Target document with version no v1.7 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at http://bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: Kermen Portable
IT Product version: v1.0
Developer`s Name: TÜBİTAK BILGEM UEKAE
Name of CCTL : TÜBİTAK BILGEM OKTEM
Assurance Package : EAL 4+ (ALC_FLR.2)
Completion date of evaluation : 03.09.2013

Kermen Portable is a software only product for file encryption in both Microsoft Windows and Pardus environments, running on a single user PC. The program requires X.509 certificates in order to perform encryption operations.

Kermen Portable implements asymmetric encryption by using EnvelopedData format defined in [RFC 5652] to ensure the confidentiality of the information. It also signs the confidential data before encrypting in order to detect any loss of integrity. The signing operation is performed again in accordance with the CMS standard defined in the [RFC 5652]. Encrypted and signed files can be decrypted and their signatures are validated by Kermen Portable according to the CMS standard.

X.509 certificates are used to identify individuals and perform asymmetric encryption. Kermen Portable checks the validity of the certificates upon encryption and decryption operations. In order a certificate to be accepted as valid by Kermen Portable, besides the other structural controls, the certificate chain must end up with a trusted certificate defined in the certificate store. The trusted certificates in the store are signed with a private key which is securely stored in a smartcard belonging to a trusted authority and the public key to validate the signature is embedded in the source code of the application which is not accessible by the user. Therefore, only the trusted authority can define which certificates will be accepted as trusted certificates. Certificate validation is performed according to the steps described in [RFC 5280].

Kermen Portable stores also the X.509 user certificates locally in its own certificate store. The private keys of asymmetric encryption and signing can be either in smartcards or in the certificate store as encrypted by user defined passwords. User is responsible for the confidentiality of the stored password. In case of smartcards, the security of the private keys is provided by the smartcards.

Kermen Portable provides a viewer for the certificate store. By using this viewer, users can view the stored certificates, import and export them if they need.

Kermen Portable does not remove the confidential data after encrypting it. The secure removal of the confidential data is out of the scope of this TOE.

TOE major security features for operational use:

- **Encryption of files:** Files are encrypted using the EnvelopedData method defined in [RFC 5652]. In EnvelopedData, data is symmetrically encrypted and the encryption key is asymmetrically encrypted for the recipients with their asymmetric public keys. The symmetric encryption algorithm is AES-CBC with a 256 bit key and asymmetric encryption algorithm is defined by the certificates of the recipients. It can be either RSA with defined key size or Elliptic Curve.
- **Integrity protection of files:** To detect the loss of integrity of data files, encrypted files are signed by the sender private key just before the encryption. For signing files, again, cryptographic message syntax is used and SignedData is created as described in [RFC **5652].** The signature algorithm is defined by the sender's public key placed in the user's signature certificate.
- **Decryption of files:** Encrypted files are decrypted if the user possesses the corresponding private key in his smart card or certificate store. Only those users who are defined as the recipient during the encryption process, can decrypt files due to the security functions of asymmetric encryption.
- **Integrity Check of files:** Since the encrypted files are also signed by the encryptor, After decrpytion of the file the result is a signed file to be validated. By this validation the inegrity of the original data file is ensured.
- **Nonrepudiation of files:** The private keys used in signing files are associated with a X.509 certificate therefore the identity of the user. By the nature of the signature operation, user can claim neither that the data is not signed by himself nor that it is modified after signing.
- **Key Storage:** Soft private keys are stored in the certificate store in password based encrypted form. For this purpose, the algorithm PBKDF2 described in [RFC 2898] (PKCS#5) is used.
- **Import/Export Keys:** Certificates and associated private keys can be imported into and exported from the certificate store by using Kermen DEPO GUI. In both cases, the user must provide the stored password.

There are 6 assumptions made in the ST regarding the development environment, production environment, initialization and maintenance environment, use environment. The ST defines one Organizational Security Policy. There is 2 threat covered by TOE and the operational environment. The assumptions, the threats and the organizational security policies are described in chapter 3 of ST in detail.

The results documented in the Evaluation Technical Report (ETR) for this product provide sufficient evidence that it meets the EAL 4 augmented with ALC_FLR.2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. CCCS declares that the Kermen portable v1.0 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the CCCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	*TSE-CCCS-016*
TOE Name and Version	*Kermen Portable v1.0*
Security Target Document Title	Kermen Portable v1.0 Security Target
Security Target Document Version	*1.7*
Security Target Document Date	*29.08.2013*
Assurance Level	EAL 4+ (ALC_FLR.2)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012
Methodology	• Common Methodology for Information Technology Security Evaluation v3.1 rev4, September 2012
Protection Profile Conformance	*No*
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, conformant • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 3, September 2012, conformant.
Sponsor and Developer	TÜBİTAK BILGEM UEKAE
Evaluation Facility	TÜBİTAK BILGEM OKTEM
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

By using Kermen Portable, two or more individuals can exchange electronic documents securely over unprotected communication paths, e.g. Networks, without risking any unauthorized persons reading the document. To achieve this, the documents are encrypted before they are sent between

the two parties, and are thus made unreadable for anyone who is not included in the recipients of the document defined by the sender.

The file encryption interface of Kermen Portable is Kermen SUR application. With Kermen SUR, after configuration, encryption of files performed by the user in just one step. Dragging the files that will be encrypted onto the application window is sufficient for encryption operation to be performed.

Likewise, in order to decrypt files that are encrypted for the user, all the user needs is to drag and drop the encrypted files onto the application window. If the user's private key stored in a smartcard then that card must be plugged in for decryption and also while encrypting, to sign the document with the user's private signing key, his or her smartcard is needed. For the keys stored in the certificate store, store password specified by the user is prompted to the user.

2.3 Assumptions and Clarification of Scope

The following conditions are assumed to exist in the TOE operational environment. These assumptions include essential environmental constraints on the secure use of the TOE. Assumptions about the intended usage of the TOE;

- The TOE runs on a single user machine with access protected by the TOE environment; i.e., only authorised users of the TOE environment may access the TOE. This includes access control provided by the operating system or equivalent and protection against malware.
- It is assumed that private keys used for decrypting and signing files are of high quality and are not disclosed to unauthorized users.
- It is assumed that passwords used for accessing the private keys in the certificate store and in the smart card are of high quality and are not disclosed to unauthorized users.
- The TOE is operated in a physically secure and well managed environment.

- The TOE user is trustworthy and trained to manage and perform encryption of classified information in accordance with any existing security policies and information classification policies. This means especially that he knows how to classify information and how to deal with, e.g., encrypting all files containing sensitive information with the appropriate key before exporting the file out of the TOE and/or its TOE environment.

- The single user PC on which the TOE is running is not connected directly to an untrusted network. This means that the PC is either assumed not to be connected to any networks or it is connected to a trusted network which is protected against attacks, so that no undocumented security critical side effects on the security functions of the TOE, which are resided in the PC, are assumed coming from this network.

2.4 Architectural Information

The target of evaluation is limited to the software application Kermen Portable, version 1.0, developed by TÜBİTAK BİLGEM. Kermen Portable consists of three parts: Kermen SUR which is a file encryption GUI, Kermen DEPO which is the viewer GUI for the certificate store and the underlying API responsible for all of the cryptographic work. API depends on Crypto++ and OpenSLL crypto libraries which are open source.

The GUI applications do only forward user request to the API and they can’t implement any cryptographic mechanism or other operations. For example, Kermen SUR’s the only job is to identify for the underlying API what operation to perform on which file. Therefore the GUI component is not security critical. In the following picture the architecture of TOE Kermen Portable and its boundaries are shown.

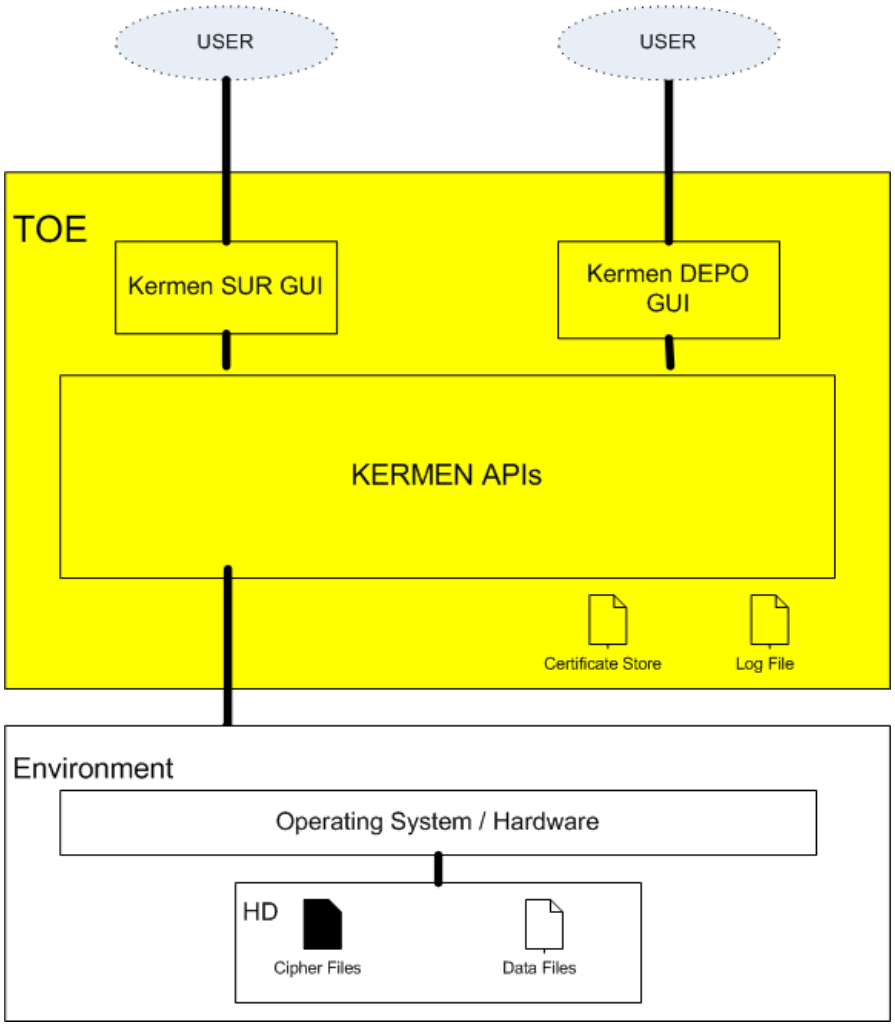

Figure : TOE Architecture and Boundaries

The physical scope of the TOE includes digital files of the application executables and APIs , user's encrypted files and log files. These files are assumed to be protected by the physical medium they are stored and by the underlying operating system.

2.5 Documentation

Kermen Portable v1.0 Security Target v1.5

Kermen Portable v1.0 Kullanım Kılavuzu v1.01

Kermen Portable v1.0 Teslim Dökümanı v1.1

2.6 IT Product Testing

Developer tests effort: Description and tests results, the developer scheduling, description and test results are documented in Kermen Portable v1.0 Test Document. The approach defined in these documents for TSFIs and depth testing is adequate to check whether the TOE behaves as described in the design documentation. The approach is oriented to test the interfaces and subsystems as they are detailed in Software Functional Specification Document, Design Document. The setup and procedures for the test cases allows demonstrating that the behavior of each subsystem is checked.

Evaluator tests effort:

Repeating Developer Tests:

- The evaluator has repeated the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report.
- The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included.

Independent Test Strategy:

- The main objective of the test performed by the evaluator is to check that the security functional requirements are implemented as expected, that the subsystems defined behave as expected, and that the TSFIs definitions are consistent with the TOE.
- The evaluator has chosen a subset of tests and an appropriate strategy for the TOE delivered by the developer. The evaluator has also considered the information coming from the security functional requirements in the security target.
- The evaluator has designed a set of tests following a suitable strategy for the TOE type.
- The evaluator has carried out tests with parameters of the TSFIs and subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed his TSFIs and subsystems independent test cases including all the security requirements defined in ST.
- All the test cases have been performed using the external interfaces that allow testing appropriately both the SFRs defined in ST and the subsystems.
- The evaluator has executed for TOE, all the tests cases defined in the independent test plan and the results obtained have been documented and referenced in this ETR.

2.7 Evaluated Configuration

The TOE configuration used in the penetration testing is consistent with the evaluated configuration according to security target

The evaluator has defined the test cases taking into account the security requirements defined in ST and the external interfaces defined in Software Functional Specifications.

Kermen Portable requires Windows XP or newer versions of Microsoft windows installed on the target machine. No installation required in order to run Kermen Portable. Only copying program files is sufficient.

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 4+ (ALC_FLR.2) as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is **PASS**. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to “ENHANCED BASIC” level attack potential attackers.

2.9 Evaluator Comments / Recommendations

Several important aspects that could influence the use of the product, taking into account the scope of the findings of the evaluation and its security target are listed;

- The TOE usage is NOT recommended given that there are exploitable vulnerabilities in the operational environment.
- The physical access to the location where the TOE is deployed must be deeply controlled to ensure that only authorized personnel have access rights.

3 *SECURITY* TARGET

The ST associated with this Certification Report is identified by the fallowing nomenclature:

Title : Kermen Portable v1.0 Security Target

Version : 1.7

Date : 29.08.2013

4 GLOSSARY

CB: Certification Body (TSE)

CC: Common Criteria

CCTL: Common Criteria Test Laboratory (TÜBİTAK BILGEM OKTEM)

CCCS: Common Criteria Certification Scheme (Turkish CC Scheme)

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

CMS: Cryptographic Message Syntax

EAL: Evaluation Assurance Level

ETR: CCTL Kermen Portable ETR (03.09.2013)

IT: Information Technology

RFC: Request for comments

STCD: Software Test and Certification department (of TSE)

ST: Security Target (Kermen Portable v1.0 Security Target v1.7)

TOE: Target of Evaluation (Kermen Portable v1.0)

TSE: Turkish Standards Institution

TSFI: TOE Security Functionality Interface

UEKAE: National Research Institude of Electronics and Cryptology of Turkey

5 BIBLIOGRAPHY

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

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[5] YTBD-01-01-TL-01 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.