Swedish Certification Body for IT Security

Certification Report - Filkrypto 1.0

Issue: 1.0, 2007-Oct-05

Responsible: Anders Staaf

Authorisation: Dag Ströman, Head of CSEC , VG CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is Filkrypto, Release 1.0.2 , developed by Tutus Data AB. Filkrypto is a one-component software application for file encryption on Microsoft Windows platforms intended to protect sensitive information in files when transmitting or storing them in unprotected environments. The TOE includes a Swedish government owned and approved cryptographic library to implement all cryptographic related and random number generator functions. Filkrypto is primarily intended for government use.

No conformance claim with any protection profile is made for the Filkrypto.

The TOE contains one function depending on a probabilistic mechanism for which a SOF claim is made in the security target. This is the integrity check at file decryption. For this function the minimum strength of function claimed is SOF-high.

No SOF claims are made for any other functions. Cryptographic verification as well as SOF analyses of the random number generation and the key derivation mechanism is performed by the Swedish NCSA government agency.

There are six assumptions made for the secure usage of the Filkrypto, two of those states that it shall be operated in a physically secure and well managed environment and that it shall not directly connect to any untrusted network. There are two threats identified, defining confidentiality and integrity violation of data files transferred over an attacked communication path. Three Organisational Security Policies states that individual encryption keys and, in case of emergency, all encryption keys shall be deleted on request of the user and that only encryption algorithm AES with 256 bit key length is allowed.

The evaluation was performed by Combitech AB in Växjö, Sweden, and was completed on 29th of August 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.3, Part 2 and Part 3, and the Common Methodology for IT Security Evaluation, CEM, Version 2.3 at Evaluation Assurance Level: EAL 3.

Combitech AB is under licensing to be an IT Security Evaluation Facility, ITSEF, within the Swedish Common Criteria Evaluation and Certification Scheme and has been granted a conditional license allowing them to perform trial evaluations under the supervision of CSEC. This evaluation served as such a trial in this licensing process. Combitech AB is also under accreditation against ISO/IEC 17025 by the Swedish accreditation body, SWEDAC.

The certifier monitored the activities of the evaluator, observed evaluation testing activities, observed the evaluator's site visit at the developer, and reviewed each work unit in all successive versions of the Single Evaluation Reports, SERs. The certifier determined that the evaluation showed that the product satisfies all functional and assurance requirements stated in the security target. The certifier concluded that the evaluator's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the evaluator in the Final Evaluation Report, FER, are consistent with the evidence produced. The evaluator concluded that the Common Criteria requirements for evaluation assurance level EAL3 have been met.

The technical information included in this report was obtained from the Security Target Filkrypto, [ST], and the final evaluation report produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the security target are met.

This Certification Report is not an endorsement of the Filkrypto product by FMV/CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the Filkrypto product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

The TOE is the file encryption application Filkrypto Release 1.0.2 and the user guidance documentation, [User].
The Filkrypto application and the user's manual are delivered on a CD-ROM marked with version number and date.

Certification Identification	
Certification ID	CSEC 2006002
Name and version of the certified IT product	Filkrypto, Release 1.0.2
Security Target Identification	Security Target, Filkrypto, Release 1.0.2, Document Version 1.3.1, 2007-10-01
Common Criteria version	2.3 as of August 2005
CEM version	2.3 as of August 2005
Evaluation Assurance Level	EAL 3
National and international interpretations	None
Scheme	The Swedish Common Criteria Evaluation and Certification Scheme under the authority of FMV/CSEC.
Sponsor and Developer	Tutus Data AB Svärdvägen 11 SE-182 33 Danderyd PoC: Per Holmer, President +46 8 551 102 30, per.holmer@tutus.se
ITSEF	Combitech AB SE-351 80 Växjö PoC: Magnus Ahlbin, Lead Evaluator +46 470 422 08, magnus.ahlbin@combitech.se
Certification Body	CSEC SE-115 88 Stockholm PoC: Anders Staaf, Lead Certifier +46 8 782 40 39, anders.staaf@fmv.se
Quality assurance, CSEC	Jerry Johansson, Certifier Dag Ströman, Technical Manager
Certification completion date	2007-10-05

3 Security Policy

The Filkrypto application provides the following three security services:

- Cryptographic Support
- User Data Protection
- Security Management

One Security Function Policy, SFP, is implemented, called K*eystore Access Control SFP*, regulating the access to the storage of the cryptographic keys.

Three organisation security policies are stated:

- P.ERASURE - Individual encryption keys shall be deleted upon the request of the authorized user.
- P.EMERGENCY - All encryption keys contained in the default keystore shall be deleted in case of emergency.
- P.ALGORITHM - The TOE shall only allow the use of approved encryption algorithms and key lengths, i.e. AES 256 bit.

3.1 Cryptographic Support

The main functions of the application are encryption, decryption and integrity protection of files.

The Filkrypto provides also means to generate, distribute, and destroy the symmetrical keys that are used by the TOE. Two types of keys are generated, one used for encryption, decryption and integrity protection of ordinary files and one type used for encryption, decryption and integrity protection of the keystores at start-up and when exporting keys from the application.

Keys can be imported from keystores and may also be manually entered into the application. The latter key type is called form keys because they are distributed on a paper form.

3.2 User Data Protection

Access to a keystore file is regulated by the policy: Keystore access control SFP. The SFP regulates that the password for accessing the keystore is chosen by the user and assigned to the keystore first. This is divided in two parts as described below.

- When starting the application the first time. The user has to choose the password for the default key store. The password is assigned to the default keystore and has to be entered each time the user wants to access the default keystore while starting the application.
- When the user wants to export keys out of the application. Here the user is as well asking to choose a password. This password has to be entered each time when a user wants to access the keystore, due to import the keys into his default keystore.

Further the SFP regulates that the access to the keystore is granted only to users providing the correct password.

3.3 Security Management

The TOE manages the following functions:

- Generate key
- Delete key

- Change keystore passwords
- Export keys
- Import keys

It also ensures that security attributes are initialised to secure values and that only secure values of the attributes are accepted.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following usage assumptions have been made in the security target, [ST].

- A.KEYDIS - It is assumed that keys used for encryption/decryption and as well as the associated keys used for integrity checks are of high quality and are not disclosed to unauthorized users. The keys are assumed to be distributed only to those parties who are authorized to use them in order to encrypt and decrypt files.
- A.FORMKEYDIS - Form keys (keys generated outside the TOE and delivered on paper) are assumed to be distributed out of band from the generating party in a secure manner, therefore they are assumed to be not disclosed and tampered during distribution. Otherwise the same assumptions apply to form keys as to keys generated in Filkrypto as described in A.KEYDIS. They are of high quality and not disclosed to unauthorized users.
- A.USER - The TOE user is trustworthy and trained to manage and perform encryption of classified information in accordance with 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.

4.2 Environmental Assumptions

The following environmetal assumptions have been done in the security target, [ST].

- A.SINGLE - The TOE runs on a single user machine, 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.
- A.PHYSICAL - The TOE is operated in a physically secure and well managed environment.
- A.CONNECT - 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.

4.3 Clarification of Scope

With the given assumptions listed above the remaining threats identified are loss of confidentiality and loss of integrity for files transferred over a communication path.

- T.DISCLOSE - An attacker of one of the communication paths over which the Filkrypto file is transferred succeeds in accessing the content of the file, i.e. the attacker violates the confidentiality of the information included in the file.
- T:TEMPER - An attacker of one of the communication paths over which the Filkrypto file is transferred tampers with the file, i.e. replacing or modifying the content of the file in a way that is not detected.

The attacker is supposed to have a very limited opportunity of attacks. For a complete description of the threats and the attacker, please see [ST], section 3 TOE Security Environment.

The Swedish NCSA provides a library of cryptographic and other mechanisms called TSAlib which is included in the FMSSL part of the Filkrypto subsystem Cryptolib, see chapter 5 Architectural Information, below. The following mechanisms from TSAlib are used:

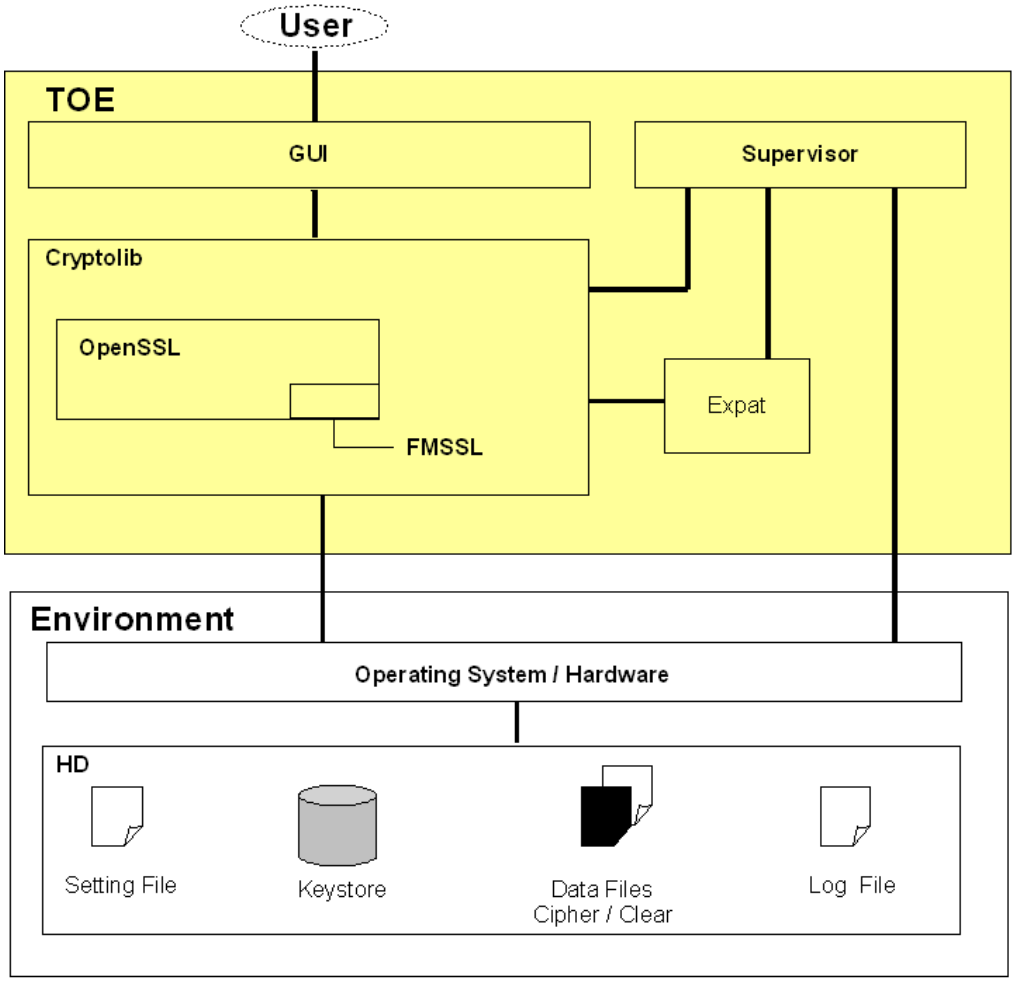
- Cryptographic encryption algorithm: AES-256
- Cryptographic hash algorithm: SHA-256 and SHA-1
- Cryptographic key generation algorithm for AES-256
- Cryptographic key destruction method
- Pseudo random number generator
- Fast pseudo random number generator for overwriting informations in files

The properties of the key generation algorithm, key destruction method and pseudo random generators are not public and no strength of function claims has been done for the cryptographic key generation or the pseudorandom function used for key derivation.

The Swedish NCSA has approved the use of and verified the correctness of the mechanisms listed above, see [CV].

5 Architectural Information

In the following picture, the architecture of Filkrypto and its boundaries are shown.



Filkrypto consists of four parts: the graphical user interface (GUI), the cryptographic library (cryptolib), the application supervisor and the XML parser (Expat). The GUI handles all user interaction and the Cryptolib all cryptographic operations, while the application supervisor handles initializations, starting, stopping, and cleanup in the application. All security critical operations are handled by the Cryptolib and the application supervisor.

Cryptolib depends on FMSSL and Expat. FMSSL is a version of the OpenSSL crypto library (http://www.openssl.org) in which all underlying cryptographic and random algorithms has been substituted by algorithms developed and approved by Swedish NCSA. Expat is an XML-parser (http://expat.sourceforge.net) used to parse the encrypted file format.

The GUI's only job is to identify to the underlying Cryptolib what operation to perform on which file. Therefore the GUI is not security critical.

6 Documentation

The following documentation is provided with the product by the developer to the customer: Filkrypto User's Manual, Release 1.0.2, 2006-11-01, Tutus Data AB.

7 IT Product Testing

The following test activities have been performed. All test results have been in accordance with the expected results.

7.1 Developer Testing

The developer testing was performed on Windows XP. Scripts running in a script-emulating environment (MinGW/MSYS) were used to automate the tests. VMware virtual machine was used for testing memory and file overwrite functions. The automated script tests were augmented with manually performed tests.
The tested version of Filkrypto was Release 1.0.2. Configuration is not applicable. The depth of the tests was on subsystem level. The tests were executed in-house at Tutus Data AB.

The developer performed tests to cover all security functions specified in the security target. The following functions have been tested for correct behaviour:

- Generation of encryption/decryption keys
- Derivation of password based keys for keystore
- Encryption and decryption of files
- Creation of HMAC
- Integrity check of files and keystores
- Import and export of keys and import of form keys
- Management functions:
  - Generate keys
  - Delete keys
  - Delete keystores
  - Change keystores password
  - Export and import keys
- The password protection of the keystores
- Emergency erase of keystores
- Erasure of residual information in memory
- Safe removal of keystore files on disk

The developer also performed a vulnerability analysis including search for known vulnerabilities in public domain sources and performed a flaw hypothesis strategy to identify potential product vulnerabilities. No residual vulnerabilities have been identified.

7.2 Evaluator Independent Testing

The evaluator independent testing was performed on Filkrypto Release 1.0.2 installed on a standard computer running Windows XP SP2. Filkrypto Release 1.0.2 was installed by following chapter 4 in [User]. Configuration is not applicable. No other equipment was installed. No resources provided by the developer were used during the execution of the tests. The tests were performed at Combitech AB in Växjö.

The evaluator's approach to identify the developer test cases to repeat was to test as many security functions as possible and to sample 20% of the developer test cases. Three of the manually performed test cases were selected.

The test approach for the evaluator's complementary independent tests was to test all security functions, to do the tests manually and to perform ten to twelve test cases, which was considered to be practical. Following the user manual the evaluator tested the following security relevant functions:

- Generation of encryption/decryption keys
- Management of passwords to keystore
- Export and import of encryption/decryption keys
- Encryption and decryption of files
- Integrity check of files
- Deletion of one and of all keys

The evaluator also performed four penetration tests to try to exploit the two vulnerabilities identified by the developer in his vulnerability analysis:

- Non-ability to erase keys
- Caching of keys on disc

The affected security functions are: SF.CLEAR and SF.MANAGE.

The evaluator came to the conclusion that neither of these vulnerabilities are exploitable which is in accordance with the developer conclusion.

8 Evaluated Configuration

The evaluated configuration is Filkrypto Release 1.0.2. The application cannot be configured. The algorithms used, key length, etc. are static parameters of the application, which can only be changed during application development.
The user can only set up in which mode, "Advanced Mode" or "Simple Mode", he wants the application to run and what he wants to be displayed in detail. The modes differ only in the provided level of guidance given to the user. The settings have nothing to do with the security configuration of the application and no additional security functionality is given in “Advanced Mode” in contrast to “Simple Mode”. The way cryptographic operations are performed is the same in both modes.

9 Results of the Evaluation

The evaluator applied each CEM work unit. When a temporary fail or inconclusive verdict where reached the developer supplied updated or complementary evidence.

The certifier reviewed the work of the evaluator, and found that sufficient evidence and justification was provided by the evaluator to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluator was justified.

One Observation Report, OR, was written by the certifier with a request to the developer and the author of the security target to clarify what parts of the external standards referenced in the security functional requirements, SFRs, that should be included in the evaluation. The security target was updated with sufficient clarifications.

The evaluation determined the Filkrypto Release 1.0.2 to be CC Part 2 conformant and to meet the CC Part 3 Evaluation Assurance Level (EAL 3) requirements.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	**Short name (including component identifier for assurance families)**	**Verdict**
Security Target	ASE	PASS
TOE Description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	ACM	PASS
CM capabilities	ACM_CAP.3	PASS
CM scope	ACM_SCP.1	PASS
Delivery and operation	ADO	PASS
Delivery	ADO_DEL.1	PASS
Installation, generation and start-up	ADO_IGS.1	PASS
Development	ADV	PASS
Functional specification	ADV_FSP.1	PASS
High-level design	ADV_HLD.2	PASS
Representation correspondence	ADV_RCR.1	PASS
Guidance	AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	ALC	PASS
Development security	ALC_DVS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testin	ATE_IND.2	PASS
Vulnerability	AVA	PASS
Misuse	AVA_MSU.1	PASS
Strength of TOE security functions	AVA_SOF.1	PASS
Vulnerability assessment	AVA_VLA.1	PASS

10 Evaluator Comments and Recommendations

The evaluator has not reported any particular considerations regarding the use of Filkrypto Release 1.0.2.

11 Security Target

The security target is identified as Security Target Filkrypto, Release 1.0.2, Document Version 1.3.1, 2007-10-01, Tutus Data AB.

12 Glossary

Glossary

(the) Scheme	The Swedish Common Criteria Evaluation and Certification Scheme.
CCRA	International arrangement to promote mutual recognition of Common Criteria certificates.
Certification	The formal approval of a product or protection profile based on the result of the evaluation.
Certification ID	Unique identifier issued by the Certification Body to clearly identify a certification.
Certification report	Report issued by the certifier at the end of each certification showing the outcome of the certification. Certification reports will be issued for all completed certifications, successful or not. The certification report is based on the final evaluation report.
Conditional license	Stage before the Evaluation Facility is granted a full license, permitting the evaluation facility to perform a trial evaluation.
Evaluation	The assessment of an IT product or protection profile against the Common Criteria using the Common Methodology to determine whether or not the security claims on the product or protection profile are justified.
Evaluation and certification scheme	The systematic organisation of the functions of evaluation and certification under the authority of a Certification Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.
Evaluation evidence	All documentation and provided information submitted by the Developer and/or Sponsor during evaluation and certification.
Evaluation facility	A non-licensed organisation that carries out independent IT product or protection profile evaluations, usually on a commercial basis. *See also* IT security evaluation facility.
Evaluation report	*See* Evaluation technical report.
Evaluation technical report	A report produced by the Evaluation Facility. Either addresses specific assurance aspects, as in the single evaluation reports, or is the final evaluation report. The final evaluation report summarises the single evaluation reports for all assessment aspects required in the Common Criteria.
Final evaluation report	Final report produced by an Evaluation Facility regarding the procedures performed and the results of evaluation of a target of evaluation. The final evaluation report summarises the single evaluation reports for all the assessment aspects required in the Common Criteria.
Full ITSEF license	After all licensing requirements are fulfilled, an Evaluation Facility is granted a full license and becomes an ITSEF.
IT security evaluation facility	An organisation licensed by the Certification Body to carry out independent IT product or protection profile

Glossary

	evaluations, usually on a commercial basis.
Licensing	Licensing of an Evaluation Facility by the Certification Body constitutes confirmation that that Evaluation Facility is qualified to perform evaluations.
Product	A package of IT software, firmware, and/or hardware providing functionality designed for use or incorporation within a multiplicity of systems.
Security target	A set of security requirements and specifications to be used as the basis for evaluation of an identified target of evaluation.
Single evaluation report	Report produced by an Evaluation Facility covering individual assurance aspects specified in the Common Criteria.
Site visit	There are several different site visits within the Scheme: auditing of the development environment of the Developer, auditing of the evaluation tests at the ITSEF, and auditing of the ITSEF during licensing. During a site visit, checks are performed as to whether the documented configuration control processes, policies, and security procedures are being applied. In addition, during a site visit to a development environment, the skills of Developers and other staff in performing tasks are assessed.
Sponsor	The organisation that applies and pays for a certification from the Certification Body.
Target of evaluation	An IT product and its associated administrator and user guidance documentation that is the subject of an evaluation.
Trial evaluation	An evaluation conducted as part of the Evaluation Facility licensing process to demonstrate technical competence and the ability of the Evaluation Facility to work in compliance with the Scheme.

Abbreviation	Description
CB	Certification Body
CC	Common Criteria (CC Part 1-3 refers to the Common Criteria standard documentation)
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation (CEM Part 1-2 refers to the CEM standard documentation)
CM	configuration management
CR	certification report
EAL	evaluation assurance level
FER	final evaluation report
FMV	Försvarets Materielverk - The Swedish Defence Material Administration
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	information technology
ITSEF	IT Security Evaluation Facility

Abbreviation	Description
OR	observation report
SER	single evaluation report
ST	security target
TOE	target of evaluation
TOR	technical oversight report

13 Bibliography

Acronym	Documents
ST	Security Target Filkrypto, Release 1.0.2, document version 1.3.1, 2007-10-01, Tutus Data AB
User	Filkrypto User's manual, Release 1.0.2, 2006-11-01, Tutus Data AB
CV	Kryptoverifiering av signalskyddssystem PGBI, HKV 12 839:73260, 2007-09-17.
CC_1	Common Criteria for Information Technology Security Evaluation, Part 1, version 2.3, August 2005, CCMB-2005-08-001
CC_2	Common Criteria for Information Technology Security Evaluation, Part 2, version 2.3, August 2005, CCMB-2005-08-002
CC_3	Common Criteria for Information Technology Security Evaluation, Part 3, version 2.3, August 2005, CCMB-2005-08-003
CEM	Common Methodology for Information Technology Security Evaluation, version 2.3, August 2005, CCMB-2005-08-004
SP-002	Evaluation and Certification, Issue: 6.0, 2007-01-22, 25550:558/05, FMV/CSEC