Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0772-2014

for

Kanguru Defender Elite 200
Kanguru Defender 2000
Universal Kanguru Local Administrator, v3.2.0.3
Kanguru Remote Management Console, v5.0.2.6

from

Kanguru Solutions

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0772-2014

Encrypted USB Storage Device

- **Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200**, Firmware Version 02.03.10, KDME200 v2.0.0.0-2/3/6,
- **Kanguru Defender 2000 with Kanguru Defender Manager 2000**, Firmware Version 02.03.10, KDM2000 v1.2.1.8-2/3/6,
- **Universal Kanguru Local Administrator**, Version 3.2.0.3 and
- **Kanguru Remote Management Console**, Version 5.0.2.6

from Kanguru Solutions

SOGIS
Recognition Agreement

PP Conformance:	Common Criteria Protection Profile for USB Storage Media, Version 1.4, 27 March 2006, BSI-PP-0025-2006
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.1

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement

Bonn, 7 November 2014

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

It includes assurance levels beyond EAL 4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2 International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product

- Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200, Firmware Version 02.03.10, KDME200 v 2.0.0.0-2, KDME200 v2.0.0.0-3, KDME200 v 2.0.0.0-6,
- Kanguru Defender 2000 with Kanguru Defender Manager 2000, Firmware Version 02.03.10, KDM2000 v 1.2.1.8-2, KDM200 v1.2.1.8-3, KDM200 v1.2.1.8-6,
- Universal Kanguru Local Administrator, Version 3.2.0.3 and
- Kanguru Remote Management Console, Version 5.0.2.6

has undergone the certification procedure at BSI.

The evaluation of the product was conducted by atsec information security GmbH. The evaluation was completed on 29 October 2014. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Kanguru Solutions.

The product was developed by: Kanguru Solutions.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

[6] Information Technology Security Evaluation Facility

5 Publication

The product

- Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200, Firmware Version 02.03.10, KDME200 v 2.0.0.0-2, KDME200 v2.0.0.0-3, KDME200 v 2.0.0.0-6,
- Kanguru Defender 2000 with Kanguru Defender Manager 2000, Firmware Version 02.03.10, KDM2000 v 1.2.1.8-2, KDM200 v1.2.1.8-3, KDM200 v1.2.1.8-6,
- Universal Kanguru Local Administrator, Version 3.2.0.3 and
- Kanguru Remote Management Console, Version 5.0.2.6

has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Kanguru Solutions
1360 Main Street
Millis, Massachusett 02054
United States

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is

- Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200, Firmware Version 02.03.10, KDME200 v 2.0.0.0-2, KDME200 v 2.0.0.0-3, KDME200 v 2.0.0.0-6,
- Kanguru Defender 2000 with Kanguru Defender Manager 2000, Firmware Version 02.03.10, KDM2000 v 1.2.1.8-2, KDM2000 v 1.2.1.8-3, KDM2000 v 1.2.1.8-6,
- Universal Kanguru Local Administrator, Version 3.2.0.3 and
- Kanguru Remote Management Console, Version 5.0.2.6.

The TOE provides protected USB mass storage. Its purpose is to protect the contents of the mass storage from unauthorized access, in case the locked storage device falls into the hands of unauthorized entities.

The USB device can be managed locally via the Universal Kanguru Local Administrator (KLA) or centrally, using the Kanguru Remote Management Console (KRMC). The KRMC allows a central administrator to control the devices in an enterprise environment.

Depending on the communication capabilities desired, the USB device is available with three different versions of the Kanguru Defender Manager (KDM[8]). The KDM/E version is identified by the version number suffix as follows: -2 (cloud version), -3 (enterprise version) or -6 (standalone version).

The protection of the user data is the major security function of the TOE. The mechanism of the protection is the complete encryption of the user data via AES-256 in CBC-mode. Its decryption, i.e. the device unlock, will only be performed if the user provides the correct password. The data protection is also robust against external disruptions, like a system crash or the power being disconnected.

When a master password is set for the device, an administrator can reset or change the user password. Resetting the user password also means deleting the user data. If a master password is to be used, it needs to be set before the user password. Otherwise, the user password will be wiped, resulting in the deletion of the user data.

The device hardware internals are covered in epoxy to provide a physical tampering protection in a way that the user will be able to detect when a tampering attempt has occurred.

The Security Target [6] is the basis for this certification. It is based on the certified Common Criteria Protection Profile for USB Storage Media, Version 1.4, 27 March 2006, BSI-PP-0025-2006 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) are outlined in the Security Target [6], chapter 6.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

[8] For Kanguru Defender Elite 200, the client application is called Kanguru Defender Manager Elite (KDME).

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
User data protection	User data on the encrypted mass storage of the USB device is protected from access when the device is locked and it can only be unlocked with the user password. All user data is stored in encrypted form, using a unique key (created via the random number generator on the device at device initialization) that is stored only on the cryptographic chip of the TOE. Only when unlocked via the user or master password, can the data be accessed and decrypted. The encrypted data is never accessible. When a master password is set, it can be used to set a new user or master password and to access the protected data. If the physical or logical connection of the unlocked device is broken, authentication is required again. The password quality has to be set according to the Evaluated Product User Guide [9], chapter 9. Brute force attacks from the client are additionally mitigated by rate limiting the password attempts to 1/s on the device.
TSF data protection	The encryption key for the protected data is stored on the device and is protected against unauthorized access. No interface exists, to extract the encryption key from within the cryptographic chip. This leaves only the potential of physical attacks. Physical attacks are blocked by the resilient nature of the TOE, as the device always returns to a locked state in case of disruptions. Additionally, the TSF enforcing chips are coated in epoxy to ensure that tamper attempts can be easily detected.
Local and remote management	Local administration can be performed by KLA, remote management via the KRMC. To use the KLA, an administrator first needs to authenticate via password. To use the KRMC, an administrator first needs to authenticate via his user ID and password. The KDM/E client is used to rely commands from the KRMC to the device. A managed device can be explicitly reset by the administrator, resulting in the deletion of the encrypted data by overwriting the encryption key with a new one. Devices can also be explicitly reset by anyone with physical access. The administrator can change his password at KLA or KRMC if needed. An administrator can trigger a reset of the user password, forcing the user to set a new one after authentication. If a master password is set, then the administrator can also change the users' password via KLA or KRMC. If a master password is to be used, it needs to be set by the administrator before the user password is set by the user. If a master password is set after a user password has been set, the user password will be wiped, which is equivalent to deleting the protected storage.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2 . Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

- Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200, Firmware Version 02.03.10, KDME200 v 2.0.0.0,
- Kanguru Defender 2000 with Kanguru Defender Manager 2000, Firmware Version 02.03.10, KDM2000 v 1.2.1.8,
- Universal Kanguru Local Administrator, Version 3.2.0.3 and

Kanguru Remote Management Console, Version 5.0.2.6.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Kanguru Defender Elite 200	-	Postal
2	HW	Kanguru Defender 2000	-	Postal
3	SW	Kanguru Defender Elite 200 Firmware	02.03.10	on Hardware
4	SW	Kanguru Defender 2000 Firmware	02.03.10	on Hardware
5	SW	Kanguru Defender Manager Elite 200 Client	2.0.0.0-2/3/6	on Hardware or Download
6	SW	Kanguru Defender Manager 2000 Client	1.2.1.8-2/3/6	on Hardware or Download
7	SW	Universal Kanguru Local Administrator SHA-256 checksum: 44f1091561ef5f4d131a0f6fd98df10dee6905c64f3bacc6e661acefa1134ae9	3.2.0.3	CD or Download
8	SW	Kanguru Remote Management Console SHA-256 checksum: 4d8fa1a41012090b0f7194a8b931e23ca79196b15a068b886bf938bf58366789	5.0.2.6	CD or Download

No	Type	Identifier	Release	Form of Delivery
9	DOC	Evaluated Product User Guide [9] SHA-256 checksum: a39c2ea831baf38983a465632c4e387652e4ab33d76c4bbe95a143fd15b974d6	1.20	Download
10	DOC	Kanguru Defender Elite 200 User Manual [10] SHA-256 checksum: 472ea7248ba2f7aab027c2006a0f9ed2644157880f6389e0a4aab39d3f75189c	1.1	Download
11	DOC	Kanguru Defender 2000 User Manual [11] SHA-256 checksum: 203119a227c17e67b3e3a84a178b7f0241b8b1274e4f9a65cde796de0d4e0d76	1.1.4	Download
12	DOC	Universal Kanguru Local Administrator User Manual [12] SHA-256 checksum: 2b2abf0f619d8c2623aed5ec973cbf1fc3c6228d8b937cd1f62f355dbcb9af65	3.2.1	Download
13	DOC	KRMC Administrator's User Manual [13] SHA-256 checksum: d79dcd21e3faa19e94dda66643aa01d2081855808fc3e2a8dd4639ed1b3547ce	5.0.2	Download

Table 2: Deliverables of the TOE

The USB device is delivered to the customer with a seal on the package, with the guidance requiring the user to verify that the seal is not broken. The USB device comes preloaded with the firmware. There are three delivery scenarios for the KDM/E client software:

- Customers (after a separate agreement with the developer) may get the device preinstalled with the CC-certified client software.
- The delivered device does not contain the CC-certified client software. The software therefore has to be updated to the CC-certified version using the downgrader application from the developer support site.
- The device, with a non-CC-certified KDM/E version installed, has already been used some time and therefore has to be migrated to the CC-certified version. For this, the device has to be updated as described in the second delivery scenario.

For the second and third scenario, the user has to verify that the device has not been tampered with before using it in the CC-evaluated configuration. For this, the following checks and operations must be performed:

- Reset the device.
- Check the checksum of the downgrader application.
- Check the checksum of the files on the device after the downgrade has been performed.

The SHA-256 checksum values for the application files after downgrading to the certified TOE version are provided in the two tables below (for KDME 200 and KDM 2000 respectively) and in Chapter 11 of the Evaluated Product User Guide [9].

File Name	SHA-256-Checksum
autorun.inf	e039edbcbd56f630a0f91b2736206a21e1654e928cf7e0e46636a3ec2a8d4fe8
enlogMacLnx.sh	90df28ab8d2b8810d3543e336c2861be2d275a4c1e8f3f540cd811efa11c32d4
enlogWin.bat	35d006f87e455a691bbbc3a06ec90eceb133d7dedac43f7145c3eb90400f57c2
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
KDMElite200.app\Contents\Info.plist	ea4f922841c1cb95f4cf6ba0ff3ec707d17fbaf32a624af09786be51de221d7d
KDMElite200.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDMElite200.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDMElite200.app\Contents\Resources\empty.lproj	-
Standard/Cloud Version 2.0.0.0-2	
Standard/Cloud (2.0.0.0-2) downgrader	3ed1c13b1f1e03024cc1401ac97d23c41dd15c10b8bef0287cfad2bb51a5a1cb
KDMElite200	7aaa053034da6862ae06f0863e716a8add8a6c6a306f0e47c35d379eb80c2b8a
KDMElite200.exe	1ae42409ee184c0c63cd8a07ceb238dc698b2b005313b65f66f57c4aee6d8bb2
version.ini (on purchase)	dce6a73d2875cef5bc07250bf017e65b297064ff4f0372e95b0ec86ada0a5ac8
version.ini (after downgrade)	a9d648bde5e1c8baa35943de0966d4066f85bb8c4c0f251d87ac4372205b3182
KDMElite200.app\Contents\MacOS\KDMElite200	a839cc84a55899dfc456e4579499274675dac15cc9fe99ca402cc241a5517923
Enterprise Version 2.0.0.0-3	
Enterprise (2.0.0.0-3) downgrader	4c12fc4313a32cee1967e7958a45c15cfb44158878d4eab21a434c78c59c389b
KDMElite200	c03eed99ad8a2e7e86e0f4cfc54c4d4746c41bfa3ee39a990471bf235d5e1c24
KDMElite200.exe	b6e69610c222d7fb5cfbb9aac2cd4ace8e5f6710e43ccaa2f2efca53fa85e49b
version.ini (on purchase)	6347a2c9ff9cb53a39f615815af4cbc165176f09cedef6e04f2678d6b054e272
version.ini (after downgrade)	892dac017567d0b8d797820fd972226f0c558711a6e99382a30b2ad46676a4a5
KDMElite200.app\Contents\MacOS\KDMElite200	f1e4c5113784f3ca459fa3083cf75a65110cd75df5958c63326cf7993341b2f6
No-Comms Version 2.0.0.0-6	
No-Comms (2.0.0.0-6) downgrader:	8686fb8267e49f2f94f7d5d4a5051467ff84390990d343597edac9c7bf83c9bb

File Name	SHA-256-Checksum
KDMElite200	129d1216a10540647e2479d4ae0ca736c66b0fab8548a1fbefa8ef406dadc7e8
KDMElite200.exe	f829fc65b315e4093ad102c7eb3e1a1140e73f45b78b29f2e3b749a8f405c0d2
version.ini (on purchase)	f11472b29d041ea434f05b2a8374b42908a63edc2e403f335199443298fa8110
version.ini (after downgrade)	65ad17a0e5a566d879ede6a3bc5581c0d1a50036cad1aa24efb87f16c7deba88
KDMElite200.app\Contents\MacOS\KDMElite200	10392d37e6e5ebcd68ef0e29b5be34fba45be0e4f6aea8837de657d3f631c9f1

Table 3: SHA-256 checksums for KDME 200 Client

File Name	SHA-256-Checksum
autorun.inf	ce93f4e4337eda6b52e0cac8eef760565ce985639aa2d4a5c58ad5f65ae5584a
enlogMacLnx.sh	bd2e68ecabd72063e875328971ffbc3980d0910d6ce34dc26d24774e5091c699
enlogWin.bat	8cc34684b6714cec9b23f5a20f7d27ddc079ec972b289d951830c355e47e5455
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
kdm2000_exec.sh	2bc65f6557d283f618ad1cfdce8771c009e91d28c14d1347386196166c34e0c1
KDM2000.app\Contents\Info.plist	3583351073de26fc9377f30f8df4c20b3ddb27cd31966347f11f27bd4689506e
KDM2000.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDM2000.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDM2000.app\Contents\Resources\empty.lproj	-
Standard/Cloud Version 1.2.1.8-2	
Standard/Cloud (1.2.1.8-2) downgrader	cbb5f4b1b3a8f3fab6c732686a2abf9cf3ba49c176686647cb2a7976ea69dff0
KDM2000	cfe4236c88133c863693555a7f77eca09a727359b700981c18c6b72d4049e115
KDM2000.exe	f6d1823e316e92bda6f1a06cf91c1f354d116106b901445897f247ced2ff5ed4
version.ini (on purchase)	eaabaed0f28dd58cec97d51b0db8334096709029525e32b0a121ab563ef23740
version.ini (after downgrade)	6fdce4d2b0a877633978dd2a54332ebd80532521a841c257950d4e0a57b05503
KDM2000.app\Contents\MacOS\KDM2000	d3d10dd417298c98a7b7e4a4e71f6b2f3c1c5ac593ad4c57b7e95a78accbbaaa
Enterprise Version 1.2.1.8-3	
Enterprise (1.2.1.8-3) downgrader	37de2a6e34a8479eab5d7f29bc2414892d81815f501df2229e6e8b38749684c3

File Name	SHA-256-Checksum
KDM2000	73e0370fd9bdfdc7bc182cc049ba4ad56939525ab2a7d2872609ef55550443d3
KDM2000.exe	ea91d11336561c6c7c605f3d41c060a53f39cdc908482f585fc98e7fee0f6bd4
version.ini (on purchase)	1b4a1a252ad6e3c13c6e621fbb35ef34934243477afc1e21b04e999f233b0a54
version.ini (after downgrade)	6fdce4d2b0a877633978dd2a54332ebd80532521a841c257950d4e0a57b05503
KDM2000.app\Contents\MacOS\KDM2000	cc4cef38f6648295fb24d342b64a7f5f5302de1dc66f3390d5b72bae95bc0e3d
No-Comms Version 1.2.1.8-6	
No-Comms (1.2.1.8-6) downgrader:	32d9f626e8965e5cbea2d924d78775fe170c9f822211f27370a7aab93d3135fb
KDM2000	8f313a05556d7b80fd84d66ff41e7414fddcdb19593c0fd3f16b202608b76a79
KDM2000.exe	6d62fa2f02b5245ec4ea15099729e7b44a6367488c2f7a14fee2a60c6a05278c
version.ini (on purchase)	cfca0dabebe27f763de9800b65c7ff670cfc51b74d4a7e84c70810b63e5bb2f1
version.ini (after downgrade)	408079e9ee7598a2e81065b6c9a0e543b14853616ef0cdd1f774acc9658b9f73
KDM2000.app\Contents\MacOS\KDM2000	50baf92470f61cee1d4511151e0af534122238d71120300305a8cbf458224cc5

Table 4: SHA-256 checksums for KDM 2000 Client

The management software KLA and KRMC is shipped via CD or can be downloaded electronically. The CDs are shipped with standard supply chain organizations (UPS, FedEx, etc). For the electronic download, HTTPS connection is used and SHA-256 checksums are provided in Table 2 above and on the download portal.

The guidance is downloaded electronically and is protected by using a HTTPS connection. The SHA-256 checksums are listed in Table 2 above and are published on the download portal.

The user can identify the hardware by the name of the model written on the device (e.g. Kanguru Defender 2000). The firmware can be identified by downloading a tool from the HTTPS secured developer download portal, which reads out the firmware version from the device. KDM/E, KLA and KRMC versions can be identified in the version.ini file on the CD-ROM partition of the device.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- User data protection
- TSF data protection
- Security management

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- There are no unauthorized attempts to access the TOE from the host system or any connected networks.
- The user takes appropriate security measures for the duration of his or her absence from the host system.
- The user ensures that it is not possible for others to see or reproduce his or her authentication attribute.
- The TOE is expected to operate in a controlled network environment.
- Those responsible for the TOE are competent and trustworthy individuals.

Users of the device check the device for evidence of physical tampering before use.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

Figure 1 shows the principal architecture of the USB storage device.

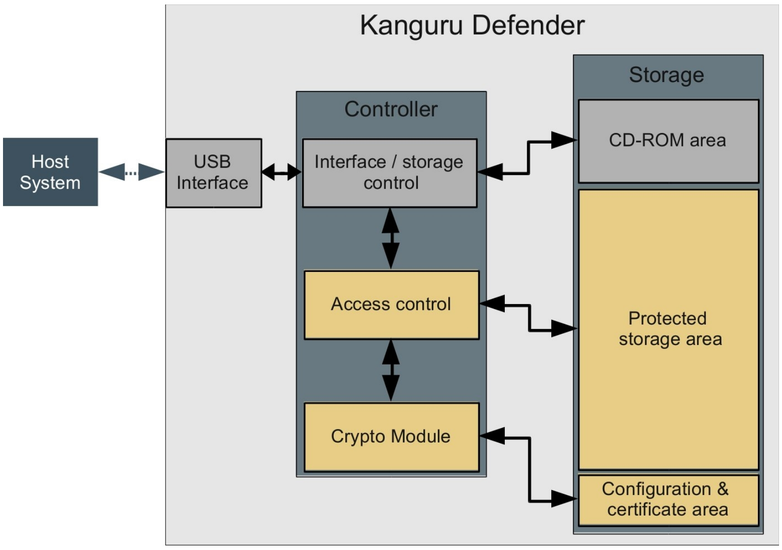

Figure 1: Device Overview

The TOE is a distributed system. The logical boundary consists of the cryptographic functionality of the device, the encrypted storage and the management software.

A standalone device is either accessed via the client application (KDM) or the KLA. An enterprise device can be additionally accessed using the remote management console (KRMC). The communication paths are shown in Figure 2.

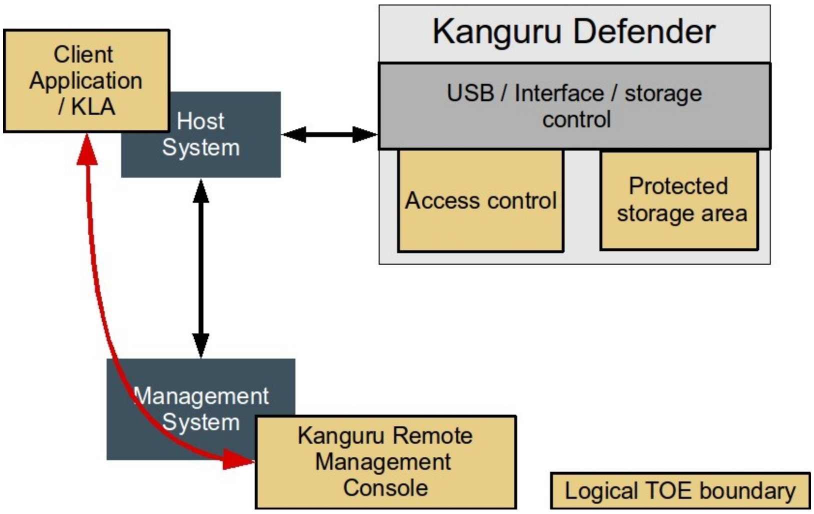

Figure 2: Logical Structure and Communication Paths

5.1 USB Device

The user interacts with the device using the client GUI software (KDM/E) that resides on the CD-ROM partition of the device. The client software is then establishing the connection with the device to authenticate the user with the given password. The device functionality is self-sustaining. It includes an own microprocessor that is run by the device firmware. There is no external interface to the processor, and only a defined SDK API interface (the interface that the software uses via USB) to the firmware. The firmware cannot be modified. The client software can be modified using the updater application from the developer's support page[9].

User data on the encrypted storage (a separate storage partition) of the device is protected from access when the device is locked and it can only be unlocked with the user password. When the device gets unlocked, the user data is decrypted with the AES key that is associated with the user's password. The AES key is stored on the device and is protected against unauthorized access.

The password and key are generated on the initialization of the device. The generation overwrites any previously existing key, effectively deleting all the user data. The same happens when performing a device reset.

There is one user and optionally one master account on a device, each having their own password. They are identical function-wise (e.g. both can unlock the protected area), except that the master account can also change the user password.

All cryptographic operations are performed by the device. The random number and key generation is performed by the firmware, while the AES encryption is implemented in hardware which is a microprocessor on the device.

The device initiates communication to the KRMC to obtain management actions prepared by the KRMC administrator.

[9] Note: Updates are not allowed in the evaluated configuration.

5.2 KLA

The KLA is a local Windows application that an administrator uses to initialize and configure devices, possibly multiple devices at the same time.

It features an administrator authentication, but the KLA administrator is not related in any way with the user accounts on the device. The KLA administrator can access the protected storage or change the user password when he has the master account password. If no master account exists, it can be set. Setting the master password also resets the user password and therefore deleting the data on the device.

KLA allows more management functions (e.g. setting password policies that get stored in the configuration & certificate area), but these do not affect the protected partition or update functionality, and are also not associated with the user/master password for accessing the protected partition. It is architecturally separated from the handling of the user data protection. Apart from the reset functionality, none of these management functions are part of the evaluated functionality.

5.3 KRMC

The KRMC is a web-based application running on an Internet Information Server. It provides administrators with password management operations (i.e. the same functions as available via KLA). The KRMC requires authentication to be used. The KRMC administrators are not related to the KLA administrator or the device users. Management operations performed on the Web GUI by the KRMC administrator do not have an immediate effect, but are only sent to the KDM of a device in the network, once the KDM asks the KRMC whether new management actions are pending. It then sends the operations (encoded as SOAP-like XML-data) to the KDM which executes the management operations on the device. The KRMC administrator cannot access the secure partition without using the master account password (the same as for KLA).

Like the KLA, the KRMC can perform additional management functions which are separated from the user data protection and user accounts on the device. Apart from the reset functionality these functions are not part of the evaluation.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer Testing

7.1.1 Test Effort

The developer tests were grouped into several test plans, one for each component (KLA, KRMC, KDM Elite 200 and KDM 2000). Each test plan contained at least 15 manual tests, each consisting of several test steps. An additional automated test suite implemented 12 test cases, each consisting of several test instructions. The tests were performed as part of the QA process to ensure that the product was ready for release. Therefore, the test case structure is systematically testing all product functions.

The developer also performed a number of so-called negative tests, to verify that the system does not allow certain actions in unexpected circumstances, e.g. using an empty password, special key input, or otherwise empty/null input on input dialogues.

7.1.2 Test Approach and Depth

The test plans have been tailored to include information on the CC-requirements (SFRs) that are covered by the tests.

The developer performed the tests on the supported platforms as follows:

- KDM/E was tested on Windows 7[10], Ubuntu 12.04, OpenSuse 11.1, Mac OS 10.7 and CentOS 4.
- KLA was tested on Windows 7.
- KRMC was tested on Windows server 2003/2008, 32/64 bit.
- The SDK API was tested from a Windows 7 Professional system.

The developer used a TSFI test mapping to ensure that all security-relevant interfaces and all SFRs have been subject to testing.

7.1.3 Test Configuration

The evaluated configuration was set up according to the Security Target [6] and the Product User Guide [9]. The developer tests showed the following combination of components for testing:

Kanguru Defender Elite 200 tests:

- Device: Kanguru Defender Elite 200
- Firmware: 02.03.10
- KDME: 2.0.0.0-2/3/6
- KLA: 3.2.0.3
- KRMC: 5.0.2.6

Kanguru Defender 2000 tests:

- Device: Kanguru Defender 2000

[10] For Windows 7 the tests were performed both as an administrative and a non-administrative user.

- Firmware: 02.03.10
- KDM: 1.2.1.8-2/3/6
- KLA: 3.2.0.3
- KRMC: 5.0.2.6

KLA tests:

- KLA: 3.2.0.3
- Tested with the Enterprise version of all device variants

KRMC tests:

- KRMC: 5.0.2.6
- KLA: 3.2.0.3
- Tested with the Enterprise version of all device variants

7.1.4 Test Results

All developer tests were run successfully.

7.2 Evaluator Testing

7.2.1 Test Effort

The evaluator reran most of the security-relevant developer tests, testing all TOE components (KDM/E, KLA, KRMC) and all device variants.

The evaluator devised and performed 16 own independent test cases including automated tests. For the automated tests, the evaluator created a test driver based on the automated tests provided by the developer.

For the cryptographic tests, a modified version of the TOE was used and the initial test code for them was adapted to include 3rd-party cryptographic verification functions.

It should be pointed out, that the TOE provides cryptographic functions that are transparent for the user and therefore the effect of those functions is not visible at the TSFI. Functional tests at the TSFI therefore would not have been able to demonstrate that those functions work as described. Although the testing requirements of ATE_COV.1 require only a testing at the TSFI (and not a coverage of all SFRs), the evaluator felt that omitting tests for the main TOE functionality, because this functionality could not be tested at the TSFI, was not a satisfactory strategy.

Yet even with the extended testing performed, a full verification that all cryptographic functions work as described was not possible. The evaluator therefore chose to perform a source code review as an additional method of testing. The approach taken allowed the evaluator to assess, that the cryptographic functions have been implemented as described in the TOE design.

7.2.2 Test Approach and Depth

The test approach was to test all interfaces and TOE components. The focus of the tests was on the authentication functions, using the SDK API provided by the firmware developer, as well as on testing the cryptographic functions. The following is a list of tested TOE functions:

- Device user and master authentication (FIA_UID.2, FIA_UAU.2, FIA_UAU.6)
- CD-ROM update verification (supports all SFRs)
- Initial password set during device initialization (FMT_MTD.1-dev)
- AES-CBC-256 encryption/decryption (FCS_COP.1)
- Key generation (FCS_CKM.1)
- DRNG output quality (FCS_RNG.1)
- Password change (FIA_UID.2, FIA_UAU.2, FDP_ACC.1, FDP_ACF.1)
- Authentication lockout including password change scenarios ((FIA_UID.2, FIA_UAU.2, FMT_MTD.1-dev, FIA_SOS.1, FMT_SMR1)
- KRMC/KLA authentication (FIA_UID.2, FIA_UAU.2)
- KRMC management commands (actions on lockout) for devices (FMT_SMF.1-POL, FMT_SMF.1)
- Device reset (FMT_SMF.1-POL, FDP_ACC.1, FDP_ACF.1)

7.2.3 Test Configuration

The evaluator applied the evaluated configuration as described in the Security Target [6] and the Product User Guide [9]. For the client platform, Windows XP was used.

In summary, the test configuration consisted of:

- KLA: v3.2.0.3
- KRMC: v5.0.2.6 (on Windows Server 2008)
- Defender Elite 200 8GB, client 2.0.0.0-3, firmware 02.03.10
- Defender 2000 4GB, client 1.2.1.8-3, firmware 02.03.10
- Defender 2000 debug devices, containing a modified firmware version, specifically designed for testing
- Windows XP host for KLA, device / client software, developer API and Defender 2000 debug device tests
- Ubuntu 12.04 for device / client software, evaluator API and Defender 2000 debug device tests
- Windows Server 2008 for KRMC tests

7.2.4 Test Results

The final tests ran successfully without any unexpected results.

Although the source code review of the firmware could not fully rule out the potential of a weak encryption or missing encryption altogether (because of the involvement of the hardware for many operations), the performed code review did not reveal anything that would be inconsistent with the expected TSF behaviour.

7.3 Penetration Testing

7.3.1 Test Effort

The evaluator performed 13 general test cases, with some tests covering different attack vectors.

For testing, the evaluator created a client (written in C) based on the SDK API. The developer client update software was also modified for these tests. Linux standard tools (strace, dd, GNU C compiler) were used to probe the behaviour and data visibility at the device level without relying on software.

The transparent encryption functionality of the TOE is not visible at the TSFI and there is no way to access the data stored in the device in order to verify that it is properly encrypted. If such a way would exist, it could itself be regarded as a vulnerability. In order to be able to perform a thorough vulnerability analysis and obtain some level of assurance that the data stored in the device is properly encrypted, the developer was required to provide significantly more information than normally would be provided for an evaluation at the EAL2 assurance level.

Even with the additional information provided, the evaluator was not able to rule out that the data stored in the device is not correctly encrypted, since direct access to the data stored in the device (i.e. by bypassing the encryption/decryption unit of the TOE) is not a function provided by the TOE. Aditionally, physically penetrating the device to obtain such access is far beyond the attack potential of an EAL2 evaluation.

7.3.2 Test Approach and Depth

The evaluator used the CVE portal and Google searches for finding publicly documented vulnerabilities. From the understanding that the evaluator gained from this, further vulnerability considerations focused on the device portion of the TOE. The general goal was to verify the device/firmware behaviour without potential interference of other TOE software, mainly to detect whether any of the security functionality is performed outside the device/firmware that might be compromised.

From the tested device functions, the evaluator focused on the encryption functionality and whether it is enforced properly or if it might be bypassed in some way.

The following list summarizes the tested areas:

- Set passwords without current password information
- SDK APIs to tamper with the TOE
- Ill-formed data input
- Default unlock code (sent by the client)
- Client-side encryption / key handling
- Weak or missing encryption of user data
- Disconnect during critical operation
- Downgrade client version
- Debug API available on TOE version
- Improper disabling of communication

7.3.3 Test Configuration

The evaluator used a sampling strategy for the tests, but made sure that all device variants were tested at least once and that the most critical tests (e.g. no plain text stored on the flash memory) were performed on all devices.

In summary, the test configuration consisted of:

- KLA: v3.2.0.3
- KRMC: v5.0.2.6 (on Windows Server 2008)
- Defender Elite 200 8GB, client 2.0.0.0-2/3/6, firmware 02.03.10 (All tests were performed with the client 2.0.0.0-3, with the exception of testing the disabling of the Cloud and KRMC communication, which was tested with 2.0.0.0-2 and 2.0.0.0-6.)
- Defender 2000 4GB, client 1.2.1.8-2/3/6, firmware 02.03.10 (All tests were performed with the client 1.2.1.8-3, with the exception of testing the disabling of the Cloud and KRMC communication, which was tested with 1.2.1.8-2 and 1.2.1.8-6.)
- Defender 2000 debug devices, containing a modified firmware version, specifically designed for testing the encryption algorithms directly
- Windows XP host for KLA, device / client software, developer API and Defender 2000 debug device tests
- Ubuntu 12.04 for device / client software, evaluator API and Defender 2000 debug device tests
- Windows Server 2008 for KRMC tests

The host system is actually less of an interest, because the critical functions are performed by the firmware inside the device.

7.3.4 Test Results

None of the penetration tests performed by the evaluator revealed an exploitable vulnerability of the TOE.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- Kanguru Defender Elite 200 with Kanguru Defender Manager Elite 200, Firmware Version 02.03.10, KDME200 v 2.0.0.0. A USB memory stick with a memory capacity of 4GB, 8GB, 16GB, 32GB, 64GB or 128GB.
- Kanguru Defender 2000 with Kanguru Defender Manager 2000, Firmware Version 02.03.10, KDM2000 v 1.2.1.8. A USB memory stick with a memory capacity of 4GB, 8GB, 16GB, 32GB, 64GB or 128GB.
- Universal Kanguru Local Administrator, Version 3.2.0.3.
- Kanguru Remote Management Console, Version 5.0.2.6.

The operational environment includes:

- Linux, MacOS or Windows (XP, Vista or Windows 7) for KDM/E
- Windows XP or newer for KLA
- Windows Server 2003 or Windows Server 2008 with MS SQL Server and IIS for KRMC

There are several functions that were not been part of the evaluation:

- Anti-Virus solution
- Write-Protect switch
- Virtualization component
- KRMC cloud

The TOE is a distributed software (when used with management functions). Its components are divided between the USB device, a local machine (which hosts the KLA or client software) and a server machine that hosts the KRMC. This is shown in Figure 2 above.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile for USB Storage Media, Version 1.4, 27 March 2006, BSI-PP-0025-2006 [7]
- for the Functionality: PP conformant
Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 2 augmented by ALC_FLR.1

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Encryption of user data in flash memory	AES-CBC	FIPS-197, NIST SP800-38A, NIST SP800-38E	256	Yes	
2	Key generation for AES encryption	HMAC_DRBG with SHA-256	SP800-90 10.1.2	N/A	N/A	

Table 5: TOE cryptographic functionality

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTPS	HyperText Transfer Protocol Secure
IIS	Microsoft Internet Information Services
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

KDM	Kanguru Defender Manager
KDME	Kanguru Defender Manager Elite
KLA	Kanguru Local Administrator
KRMC	Kanguru Remote Management Console
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, September 2009

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[11].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0772-2014, Version 1.10, 2014-10-06, Kanguru Defender Security Target, Kanguru Solutions

[7] Common Criteria Protection Profile for USB Storage Media, Version 1.4, 27 March 2006, BSI-PP-0025-2006

[8] Evaluation Technical Report, Version 8, 2014-10-07, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[9] Evaluated Product User Guide, Version 1.20, 2014-10-02

[10] Kanguru Defender Elite 200 User Manual, Version 1.1, 2014-08-27

[11] Kanguru Defender 2000 User Manual, Version 1.1.4, 2014-08-27

[12] Universal Kanguru Local Administrator User Manual, Version 3.2.1, 2013-08-03

[13] KRMC Administrator's User Manual, Version 5.0.2, 2013-11-01

[14] Configuration lists for the TOE (confidential documents):

a) Configuration list for TOE executables, 2014-09-17

b) Configuration list from Phison, 2014-09-17

c) Configuration list for downgrader description, 2014-09-17

d) Configuration list for Secure FTP, 2014-10-06

e) Configuration list for design evidence, 2014-09-17

f) Configuration list for user documentation, 2014-10-02

g) Configuration list for test evidence, 2014-09-15

h) Kanguru hardware configuration setup file, 2014-09-17

i) Kanguru JIRA Bug Report, 2014-09-16

[11] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

"The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D."

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.