# Certification Report

## EAL 2 Evaluation of

## Tamara Elektronik Ltd.Şti.
## USBK Cryptobridge v2.0 For Model A101 and Model A103

issued by

**Turkish Standards Institution**
**Common Criteria Certification Scheme**

| | |
|---|---|
| **Date** | **: 12.10.2011** |
| **Pages** | **: 24** |
| **Certification Report Number** | **: 14.10.01/11-401** |

*This page left blank on purpose*.

----- o -----

# TABLE OF CONTENTS:

## LIST OF TABLES

## FIGURES

*This page left blank on purpose.*

----- o -----

## CERTIFICATION REPORT

The Certification Report is drawn up to submit the Certification Committee the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme.

Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

# 1. INTRODUCTION

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

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited with respect to that standard by the Turkish Accreditation Agency (TÜRKAK), the national accreditation body in Turkey. The evaluation and tests related with the concerned product have been performed by TÜBİTAK-BİLGEM-UEKAE-OKTEM, which is a public CCTL.

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

This certification report is associated with the Common Criteria Certificate issued by the CCCS for **USBK Cryptobridge v2.0 For Model A101 and Model A103** whose evaluation was completed on 23.09.2011 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the Security Target document with version no 09 of the relevant product.

## 2. GLOSSARY

| | |
|---|---|
| **CCCS:** | Common Criteria Certification Scheme |
| **CCTL:** | Common Criteria Test Laboratory |
| **CCMB:** | Common Criteria Management Board |
| **CEM:** | Common Evaluation Methodology |
| **ETR:** | Evaluation Technical Report |
| **IT:** | Information Technology |
| **OKTEM:** | Common Criteria Test Center (as CCTL) |
| **PCC:** | Product Certification Center |
| **ST:** | Security Target |
| **TOE:** | Target of Evaluation |
| **TSF:** | TOE Security Function |
| **TSFI:** | TSF Interface |
| **SFR:** | Security Functional Requirement |
| **TÜBİTAK:** | Turkish Scientific and Technological Research Council |
| **TÜRKAK:** | Turkish Accreditation Agency |
| **BİLGEM:** | Center of Research For Advanced Technologies of Informatics and Information Security |
| **UEKAE:** | National Electronics and Cryptology Research Institute |
| **EAL:** | Evaluation Assurance Level |
| **PP:** | Protection Profile |
| **AES:** | Advanced Encryption Standard |
| **SCSI:** | Small Computer System Interface |
| **MSD:** | Mass Storage Device |
| **LUN:** | Logical Unit Number |
| **FIPS:** | Federal Information Processing Standard |
| **RTOS:** | Real-time Operating System |
| **USB:** | Universal Serial Bus |

**Table 1 - Glossary**

# 3. EXECUTIVE SUMMARY

**Evaluated IT product name:**

USBK Cryptobridge v2.0 For Model A101 and Model A103

**IT Product version:**

v2.0 For Model A101 and Model A103

**Developer`s Name:**

Tamara Elektronik Ltd.Şti.

**Name of CCTL :**

TÜBİTAK BİLGEM UEKAE OKTEM Common Criteria Test Laboratory

**Completion date of evaluation :**

23.09.2011

**Common Criteria Standard version :**

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009

**Common Criteria Evaluation Method version :**

- Common Methodology for Information Technology Security Evaluation v3.1 rev3, July 2009

## Short summary of the Report:

1) **Assurance Package :**

   EAL 2

2) **Functionality :**

USBK Cryptobridge, the TOE, is a disk encryption product which the users have the ability to encrypt/decrypt all data transmitted between host system and a back disk. Since the main feature of the TOE is encrypting/decrypting the transmitted data from/to the TOE, the users of the TOE are not restricted with a limited disk space, on the contrary, they have the ability to use TOE with any USB flash drives and USB external harddrives which can be plugged to the TOE.

The TOE is also not dependent to any operating system on the host system which the encrypted data will be transmitted from. The TOE communicate with the host system with Small Computer System Interface (SCSI). TOE is supporting predefined vendor specific SCSI commands. An application on the host system can be used as an interface between user and SCSI. This type of communication between host system and TOE provides independence from the operating system.

For MS Windows Operating Systems the application is provided by TOE, for other type of Operating Systems vendor will provide the installation file through the vendor website.
On the other hand, the TOE will also support another interface for managing the TOE functionality through a simple text editor. This methodology can be used for the operating systems for which an application in the vendor website is not provided.
TOE is delivered to its customers with two different models called Model A101 and Model A103 provide the opportunity to use single cryptographic key where Model A103 support up to three keys. The customers of Model A103, select the key during activation and use TOE according to its operational guidance and on the other hand Model A101 use the only key supported by TOE. All the security functionalities defined in this ST are both valid for two TOE models as well as the assurance measures.

TOE supports cryptographic operation according to the supported AES key size. The users of the TOE can either generate a 128-bit or 256-bit AES key.

## 3) Summary of Threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product:

**Subjects:**

| Subjects | Description |
|---|---|
| U.OWNER | The Authorized User |
| U.BADMAN | A Threat Agent that has a chance of use USBK and Back disk of real owner (user). This agent may be any kind of person, malware, virus, trojan, worm, etc. |
| U.CRYPTANALYST | A Threat Agent that has plenty of cryptographic knowledge. This agent can get the Back disk and try to decrypt the content (ie User Data).<br>This agent can get residueal of erasure Flash memory of TOE and try to decrypt the content (i.e. User Security Attributes). |
| U.HARDANALYST | A Threat Agent that has plenty of hardware knowledge. This agent probes the USBK hardware and tries to read the security attributes. |
| U.NATURALCAUSE | A Threat Agent that has a plenty of energy to change the bits of firmware. |

**Table 2- Subjects**

The TOE counter such threats presented in the table below and provides functions for countermeasure to them.

| Threats | Description |
|---|---|
| T.UNAUTHORISED | U.BADMAN can gain access to the user data on Back disk by activating TOE with correct password. TOE can not recognise the difference between U.OWNER and U.BADMAN since either provides correct password. |
| T.PROBING_NON-VOLATILE MEMORY | U.HARDANALYST can reveal the transfer key(s), user password by probing the non-volatile memory on the integrated circuit. |
| T.PROBING_PROGRAM MEMORY | U.HARDANALYST can reveal the storage key by probing the program memory on the integrated circuit. |
| T.CORRUPTION | The integrity of user security attributes and firmware might be corrupted by U.NATURALCAUSE . |

**Table 3 - Threats**

## 4) Special Configuration Requirements:

TOE should be configured before the usage in a host system with the following minimum configuration;

- USB host interface,
- MSD class drivers with multiple LUN support,
- FAT16 file system,
- Text editor,
- A display and I/O unit.

TOE can be used in any host system with a USB interface and MSD driver and can encrypt the transmitted data to any external drive with USB interface.

## 5) Assumptions about the Operating Environment:

| Assumptions | Description |
|---|---|
| A.USER | U.OWNER should protect their security attributes (user passwords, transfer keys) from disclosure. He/she is aware of the value of his/her data and is strongly intented to protect it. |
| A.HOST | Operational environment should be protected against virus, trojan, malware or any type of network attacks which can compromise the security of data transfer between the host system and TOE. Operational environment should also be trusted. |
| A.OPERATIONAL ENVIRONMENT | Operational environment does not allow an attacker to access the back disk when sensitive data is accessible to rightful user on the host system. |
| A.AUTOACTIVATION | Users should physically protect the TOE if they set the auto activation state “on”. |

**Table 4 – Assumptions**

## 6) Disclaimers:

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1 ,revision 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

## 4. IDENTIFICATION

TOE is an integrated system which provides users to protect their data after the transmission to a back disk. The components of TOE are integrated with a vendor specific firmware which enforce encrypt/decrypt operations during data transfer.

Upon the initialisation and activation of the TOE, the authorized user can transfer data by encrypting it with a 128-bit or 256- bit AES transfer key, according to his/her choice, to a formatted back disk. Also authorized user can perform the decryption operation for the encrypted files in a back disk.

The user can configure the security functions and user security attributes of the TOE only if the TOE is deactivated. Appropriate user authentication is performed during configuration.
Two different models of TOE can be used which the only difference is the number of supported transfer keys. One of the model is supporting only one transfer key and the other is supporting three different transfer keys.

The firmware is the same for both models of TOE. Only difference is the global setting-NumberOfKeys- that can be 1 or 3. Firmware acts according to this setting.
During the activation selection of the transfer key is supported to the user. But for TOE model A101, there is no chance other than 1.

The following figure is showing the generic usage of the TOE

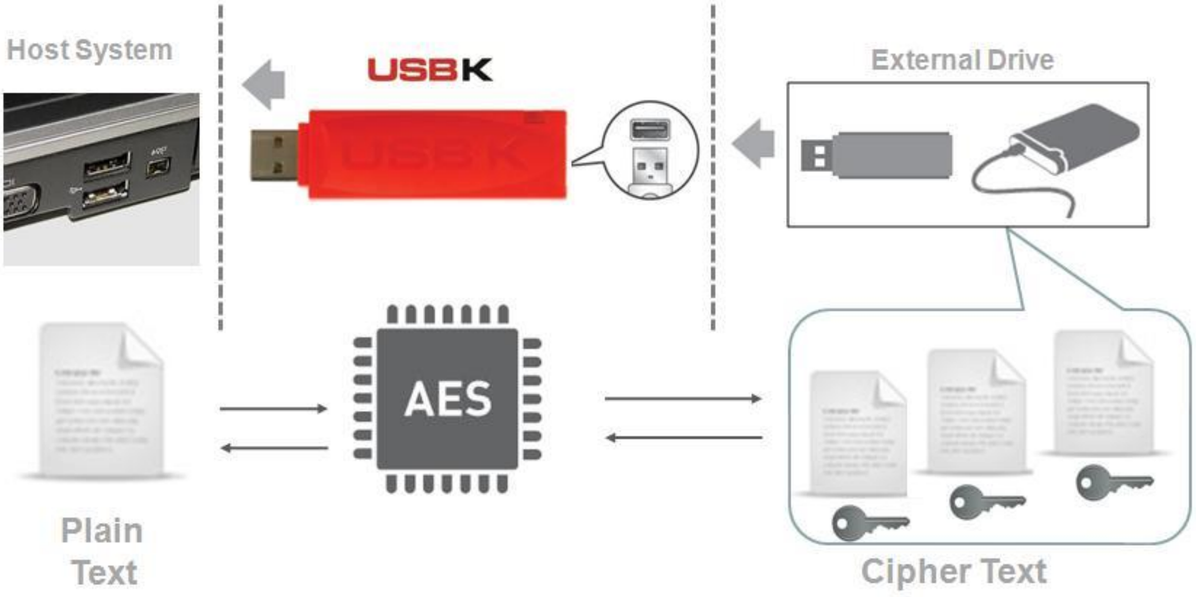

**Figure 1 - Generic Usage of the TOE**

**Initial State of TOE;**

The TOE can be assumed in initial state in three conditions. Either when the user purchase the TOE first time, after the retry number dropped to zero or after user data integrity is lost.

At initial state, transfer key(s) have been randomly generated by TOE.

At initial state, TOE enforce the user to provide user password. All other management functions are inaccessible before setting the user password.

**Deactivate State of TOE - Configuring the TOE;**

The user can change the following settings;

- User password,
- Transfer key(s),
- Auto-activation value,

The user can assign names for the following;

- Transfer key(s),
- Device,

TOE will request authorization for each operation defined above.

**Activate State of TOE - Normal Usage;**

Transfer functionality of the TOE will be activated by user after selecting the key with correct user password.

The user can plug a back disk to the TOE. Host system will recognize the back disk as decrypted. If the back disk is used for the first time with the active key of TOE, operating system will announce that back disk is unformatted. The user can transfer the data encrypted right after formatting the disk.

Transfer session with the back disk will be terminated upon deactivation.

File system information and user data stored in the back disk is always encrypted with 128-bit or 256-bit AES key which is user defined at setting and selected at activation.

Users of the TOE can configure the TOE as auto activated. With this settings, preselected transfer key is activated automatically. This feature is provided for integration with host systems without any interface for user authorization such as testing equipments.

**Programming Mode of TOE**

TOE is taken into programming mode when firmware upgrade is required.

TOE itself also goes into programming mode when it detects corruption in firmware.

## 5. SECURITY POLICY

### Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

| Policy | Description |
|---|---|
| OSP.CRYPTANALYSIS | The cryptographic keys (transfer keys) , on which cryptographic algoritms depends, must be sufficiently strong to protect encrypted user data againts trial of U.CRYPTOANALYST. U.OWNER should take responsibility. TOE can generate random keys for U.OWNER. TOE implements AES as cryptographic algorithm which is mathematically strong against cryptanalysis. |

**Table 5 – Organizational Security Policy**

## 6. ARCHITECTURAL INFORMATION

### Physical Scope

The following figures are showing the physical scope of the TOE and interface between the modules and TOE units.

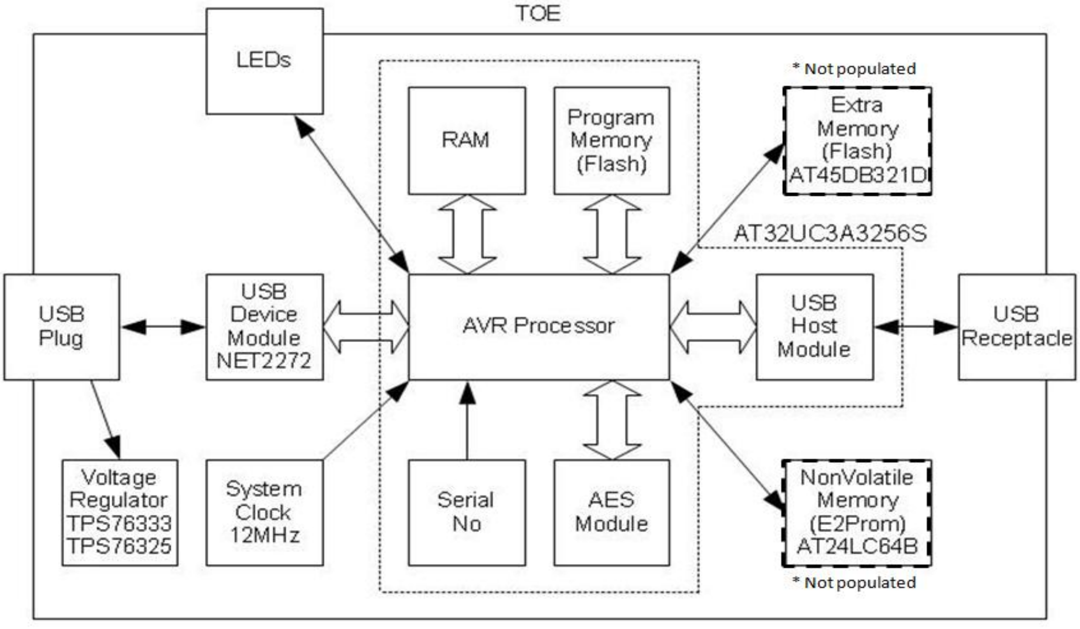

**Figure 2-Physical Scope of the TOE**

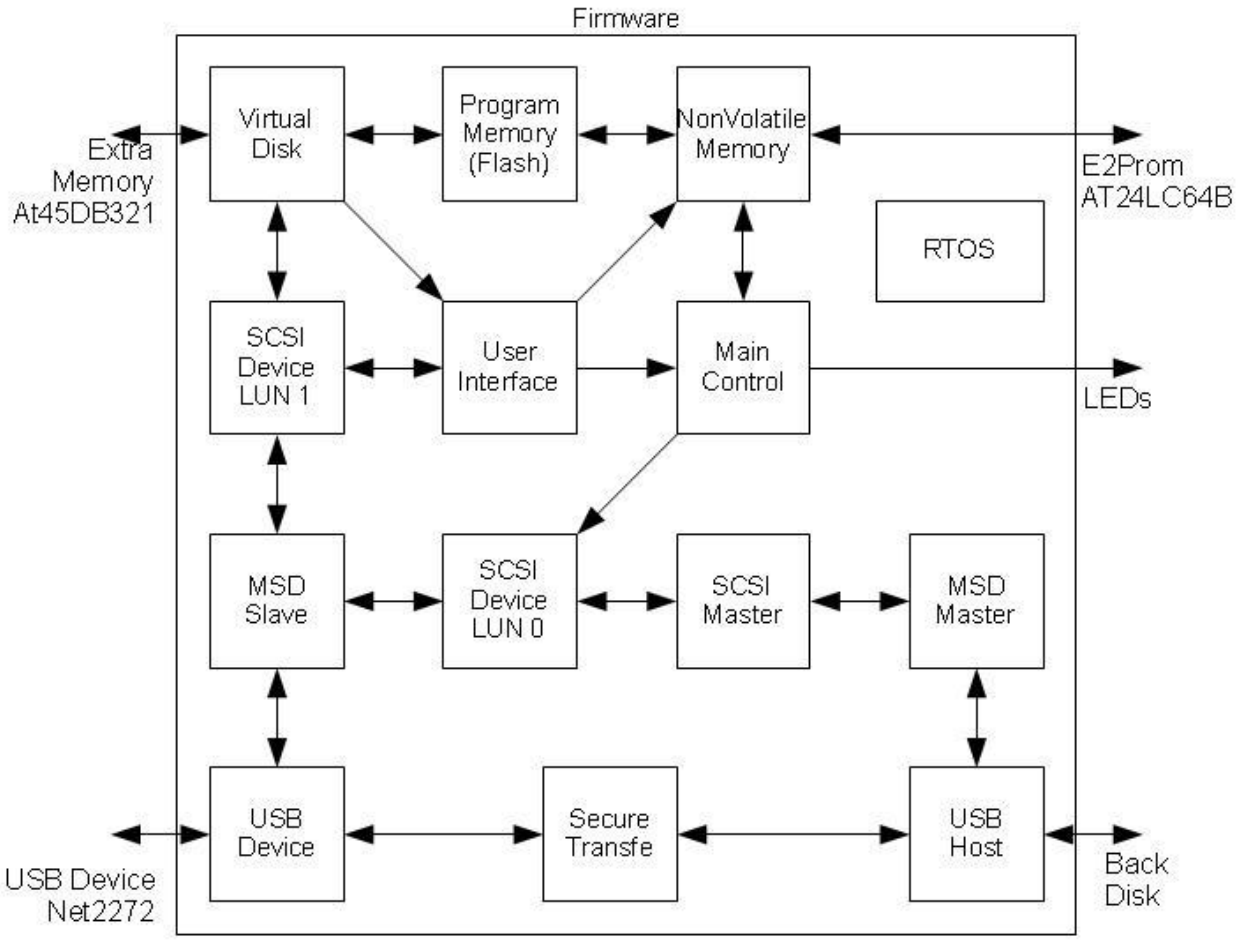

**Figure 3-Firmware View of Physical Scope for TOE**

TOE consists of hardware module and firmware module. Hardware provides an execution environment for the firmware. Program is placed in program memory (Flash) and executed on RAM by AVR processor. All of them are in the microcontroller module.
Further details on these modules are found in Section 1.4.1 of the ST.

## Logical Scope

**Cryptography:** TOE provides the following two types of cryptographic operation with AES algorithm;

- Encryption/Decryption of user security attributes: Encryption/Decryption of user security attributes (user password and transfer key) into non-volatile memory by encrypting with

256-bit AES storage key. This storage key is generated randomly during first run of the firmware. The storage key is generated once and used during the life-cycle of the firmware.

- Encryption/Decryption of user data: Encryption/Decryption of transferred data between host system and back disk by using 128-bit or 256-bit AES transfer key according to user selection during definition of transfer key(s). Initially TOE fills transfer key(s) with randomly generated 256-bit one(s) and user is able to change them during setting up of TOE. User may make TOE generate random 128-bit or 256-bit AES key in order to get a stronger key. User data, encrypted/decrypted during this cryptographic operation includes both user files and file system information.

**Data Protection:** TOE provides data protection and confidentiality of user data by encrypting the data on the fly with AES algorithm. TOE also protect user security attributes by encrypting them with AES algorithm. TOE does not allow reading program memory which contains security attributes of user and TOE. This access is only valid after the erasure of the program memory. TOE also provides integrity of user security attributes and program memory by cycling redundancy check (CRC).

**Authentication:** TOE enforces users to provide password for each operation requests except deactivation.

**Management:** TOE allows users to change/set values for the parameters below;

- auto activation,
- user password,
- transfer key,
- device label,
- transfer key label

**Testing:** During the start-up of TOE, the following self tests are conducted;

- CRC check for program memory and user security attributes,
- Control of AES encryption/decryption operations,
- Control of communication bus within the TOE,

**Resource Utilisation:** User security attributes are encrypted and stored with a back up copy. According to the result of CRC checking, the back up copy of user security attributes will be overwritten to the corrupted one.

# 7. ASSUMPTIONS AND CLARIFICATION OF SCOPE

TOE consists of the components which are defined in section 6 (Architectural information). Except these, Other components are not in the scope of Common Criteria Evaluation.

## 7.1 Usage Assumptions

| Assumptions | Description |
|---|---|
| A.USER | U.OWNER should protect their security attributes (user passwords, transfer keys) from disclosure. He/she is aware of the value of his/her data and is strongly intented to protect it. |
| A.AUTOACTIVATION | Users should physically protect the TOE if they set the auto activation state “on”. |

**Table 6-Usage Assumptions**

## 7.2 Environmental Assumptions

| Assumptions | Description |
|---|---|
| A.HOST | Operational environment should be protected against virus, trojan, malware or any type of network attacks which can compromise the security of data transfer between the host system and TOE. Operational environment should also be trusted. |
| A.OPERATIONAL ENVIRONMENT | Operational environment does not allow an attacker to access the back disk when sensitive data is accessible to rightful user on the host system. |

**Table 7-Enviromental Assumptions**

## 7.3 Clarification of Scope

Under normal conditions; there are no threats which TOE must counter but did not; however Operational Environment and Organizational Policies has countered. Information about threats that are countered by TOE and Operational Environmental are stated in the Security Target document.

## 8. DOCUMENTATION

USBK Cryptobridge v2.0 Security Target Document
Version Number and Date: v0.9, 22.08.2011

USBK Cryptobridge v2.0 Administrator and User Guidance Document , EN
Version Number and Date: v1.6, 23.09.2011

USBK Cryptobridge v2.0 Administrator and User Guidance Document , TR
Version Number and Date: v1.2, 23.09.2011

## 9. IT PRODUCT TESTING

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences are mapped to the assurance families of Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the Evaluation Technical Report (ETR) of USBK Cryptobridge v2.0 For Model A101 and A103.

It is concluded that the TOE supports EAL 2. There are 19 assurance families which are all evaluated with the methods detailed in the ETR.

**IT Product Testing is mainly realized in two parts:**

**1) Developer Testing :**

- **TOE Test Coverage**: Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE Test Document according to the TOE Design documentation which include TSF subsystems and its interactions.
- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

**2) Evaluator Testing :**

- **Independent Testing:** Evaluator has done a total of 28 sample independent tests. 21 of them are selected from developer`s test plans. The other 7 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- **Penetration Testing:** Evaluator has done 5 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in the ETR and the penetration tests and their results are available in detail in the ETR document as well.

**The result of AVA_VAN.2 evaluation is given below:**

- It is determined that TOE, in its operational environment, is resistant to an attacker possessing **"Basic"** attack potential.

For the product USBK Cryptobridge v2.0 For Model A101 and A103, there is no residual vulnerability (vulnerabilities can be used as evil actions by the hostile entities who have **ENHANCED BASIC, MEDIUM ve HIGH** level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

## 10. EVALUATED CONFIGURATION

During the evaluation; the configuration of evaluation evidences are shown below:

**Evaluation Evidence :** TOE – USBK Cryptobridge v2.0
Version Number : v2.0

**Evaluation Evidence :** USBK Cryptobridge v2.0 Basic Design Document
(Temel Tasarım Dökümanı)
Version Number and Date: v0.4, 23.08.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Functional Specification Document
(Fonksiyonel Belirtim Dokümanı)
Version Number and Date: v0.6, 23.08.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Security Architecture Document
(Güvenli Mimari Dokümanı)
Version Number and Date: v0.3, 16.05.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Delivery and Usage Document
(Teslim ve İşletim Dokümanı)
Version Number and Date: v0.3, 04.04.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Configuration Management Plan
(Konfigürasyon Yönetim Planı)
Version Number and Date: v0.1, 23.03.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Preperative Procedures
(Kurulum Prosedürleri Dokümanı)
Version Number and Date: v0.1, 24.03.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Configuration Features List
(Konfigürasyon Öğeleri Listesi)
Version Number and Date: v0.1, 23.03.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Security Target Document
(Security Target Dokümanı)
Version Number and Date: v0.9, 22.08.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Test Document
(Test Dokümanı)
Version Number and Date: v0.17, 13.09.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Administrator and User Guidance Document , EN
(Yönetici ve Kullanıcı Kılavuzu Dokümanı)

Version Number and Date: v1.6, 23.09.2011

**Evaluation Evidence :** USBK Cryptobridge v2.0 Administrator and User Guidance Document , TR (Yönetici ve Kullanıcı Kılavuzu Dokümanı)
Version Number and Date: v1.2, 23.09.2011

## 11. RESULTS OF THE EVALUATION

Table 8 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 2 (EAL 2) components as specified in Part 3 of the Common Criteria.

| Component ID | Component Title |
|---|---|
| ASE_INT.1 | ST Introduction |
| ASE_CCL.1 | Conformance Claims |
| ASE_SPD.1 | Security Problem Definition |
| ASE_OBJ.2 | Security Objectives |
| ASE_ECD.1 | Extended Components Definition |
| ASE_REQ.2 | Security Requirements |
| ASE_TSS.1 | TOE Summary Specifiation |
| ADV_ARC.1 | Security Architecture |
| ADV_FSP.2 | Functional Specification |
| ADV_TDS.1 | TOE Design |
| AGD_OPE.1 | Operational User Guidance |
| AGD_PRE.1 | Preparative Procedures |
| ALC_CMC.2 | Configuration Management Capabilities |
| ALC_CMS.2 | Configuration Management Scope |
| ALC_DEL.1 | Delivery |
| ATE_COV.1 | Coverage |
| ATE_FUN.1 | Functional Tests |
| ATE_IND.2 | Independent Testing |
| AVA_VAN.2 | Vulnerability Analysis |

**Table 8 - Security Assurance Requirements for the TOE**

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE USBK Cryptobridge v2.0 For Model A101 and A103 the result of the assessment of all evaluation tasks are “Pass”.

**Results of the evaluation:**

USBK Cryptobridge v2.0 For Model A101 and A103 product was found to fulfill the Common Criteria requirements for each of 19 assurance families and provide the assurance level EAL 2. This result shows that TOE is resistant against the "BASIC'' level attack potential and it countervails the claims of the functional and assurance requirements which are defined in ST document.

**There is no residual vulnerability** (vulnerabilities can be used as evil actions by the hostile entities who have ENHANCED BASIC, MEDIUM ve HIGH level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

## 12. EVALUATOR COMMENTS/ RECOMMENDATIONS

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of USBK Cryptobridge v2.0 for model A101 and A103 product, result of the evaluation, or the ETR.

## 13. CERTIFICATION AUTHORITY COMMENTS/ RECOMMENDATIONS

The certifier has no comments or recommendations related to the evaluation process of USBK Cryptobridge v2.0 for model A101 and A103 product, result of the evaluation, or the ETR.

## 14.SECURITY TARGET

Information about the Security Target document associated with this certification report is as follows:

**Name of Document :** USBK Cryptobridge v2.0 Security Target
**Version No :** 0.9
**Date of Document :** 22.08.2011

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

## 15. BIBLIOGRAPHY

1) Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009

2) Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009

3) USBK Cryptobridge v2.0 Security Target Version: 0.9 Date: 22.09.2011

4) Evaluation Technical Report (Document Code: DTR 17 TR 01), October 11, 2011

5) PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

## 16. APPENDICES

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