COMMON CRITERIA RECOGNITION ARRANGEMENT
FOR COMPONENTS UP TO EAL 4

Certification Report

EAL 4+ (AVA_VAN.5)

Evaluation of
TÜBİTAK BİLGEM UEKAE
UKİS (NATIONAL SMART CARD OPERATING SYSTEM)
v1.2.2 ON UKT23T64H v4

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	04.09.2012
Version of Report	1.0
Author	Mehmet Kürşad ÜNAL
Technical Responsible	Mariye UMAY AKKAYA
Approved	Fatih ÇETİN
Date Approved	04.09.2012
Certification Report Number	14.10.01/2012-312
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Lab	TÜBİTAK BİLGEM OKTEM Common Criteria Test Laboratory
TOE	UKİS (National Smart Card Operating System) v1.2.2 on UKT23T64H v4
Pages	17

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1.0	04.09.2012	All	Final Relased

DISCLAIMER

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

FOREWORD

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

The Common Criteria Certification Scheme (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 by accreditation bodies (TÜRKAK). The evaluation and tests related with the concerned product have been performed by TÜBİTAK-BİLGEM-OKTEM*, which is a public/commercial 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 UKT23T64H v4 üzerinde UKİS (ULUSAL AKILLI KART İŞLETİM SİSTEMİ) v1.2.2-UKİS (NATIONAL SMART CARD OPERATING SYSTEM) v1.2.2 on UKT23T64H V4 whose evaluation was completed on 30.06.2012 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the Security Target document with version no 20 of the relevant product.

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

RECOGNITION OF THE CERTIFICATE

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

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

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

The Target of Evaluation is contact based smart card which is called UKİS (National Smart Card Operating System) v1.2.2 on UKT23T64H v4. The TOE is comprised of hardware and software. The hardware UKTÜM IC UKT23T64H v4 is certified according to CC EAL5+ (AVA_VAN.5) by Turkish CC Scheme with the certificate number "TSE-CCCS-010".

The communication of the TOE is provided over the smart card reader or access device such as POS (Point of Sale) machine. The PC sends commands over the smart card reader or POS and the smart card responses to the PC over the smart card reader or POS back.

The TOE has 8 pins according to the IEC/ISO 7816-2. The I/O pin is used for communication. The other pins are VCC, GND, RST and CLK and the remaining two are reserved for future use. As mentioned before TOE is comprised of hardware UKTUM IC UKT23T64H v4 and operating system (UKİS). The operating system specifications of the TOE are as follows:

- Embedded software (UKİS) of the TOE is loaded into ROM of the UEKAE's secure Smart Card chip UKT23T64H v4,
- Communicates with the PC via card reader according to ISO/IEC 7816-4 T = 1 protocol,
- Implements user and interface authentication,
- Manage the various kinds of data files stored in the non-volatile EEPROM memory
  - It is capable of binary file operations (open, update, erase, read),
  - Supports fixed length linear, variable length linear, fixed length cyclic file structures and file operations (open, append record, update record, read record),
  - Provides access control of the files if required, by the configuration
- Follows the life cycles (activation, manufacturing, initialization, personalization, administration, operation and death) and operates functions according to the present life cycle,
- Does not allow loading of executable files,
- Encrypts, decrypts, digitally signs and verifies with RSA/DES/3DES/AES cryptographic algorithms by using HW modules of the UKTÜM,
- Calculates SHA-1 hash.

As a smart card having the specifications above, the TOE can be used as PKI card (for digital sign), personal identification card and health care card.

The hardware UKTÜM IC UKT23T64H v4 comprises of 8051 CPU, 64K ROM, 64K NVM, 8K External RAM, UART, Timers, ACE (Advanced Crypto Engine) ,RNG (Random Number Generator), Security Sensors, IC dedicated library functions. UKTÜM UKT23T64H v4 has CC EAL 5+ (AVA_VAN.5) certificate (Turkish CC Scheme with the certificate "TSE-CCCS-010"). UKİS v1.2.2 Operating System is loaded into the ROM of the UKTÜM chip during the manufacturing of IC. The more knowledge about the IC can be found its security target document.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	TSE-CCCS-011
TOE Name and Version	UKİS (NATIONAL SMART CARD OPERATING SYSTEM) v 1.2.2 on UKT23T64H v4
Security Target Document Title	UKİS (NATIONAL SMART CARD OPERATING SYSTEM) V1.2.2 ON UKT23T64H v4
Security Target Document Version	20
Security Target Document Date	07.08.2012
Assurance Level	EAL 4+ (AVA_VAN.5)
Criteria	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
Methodology	Common Methodology for Information Technology Security Evaluation v3.1, rev 3, July 2009
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package Conformant to EAL4+(AVA_VAN.5)
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Facility	TÜBİTAK BİLGEM OKTEM Common Criteria Test Laboratory
Certification Scheme	Turkish Standard Institution Common Criteria Certification Scheme

2.2 Security Policy

The TOE does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

This section describes the assumptions that must be satisfied by the TOE operational environment.

A.DLV_CONTROL	Procedures must guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following secure usage assumptions. Secure storage and handling procedures are applicable for all TOE's parts (programs, data, documents, etc).
A.DLV_CONF	Procedures must also prevent if applicable any non-conformance to the confidentiality convention and must have a corrective action system in case any non-conformance or misprocessed procedures are identified.
A.DLV_PROTECT	Procedures shall ensure protection of material/information under delivery including the following objectives: • non-disclosure of any security relevant information, • identification of the elements under delivery, • meeting confidentiality rules (confidentiality level, transmittal form, reception acknowledgment), physical protection to prevent external damage.
A.DLV_TRANS	Procedures shall ensure that material/information is delivered to the correct party.
A.DLV_TRACE	Procedures shall ensure traceability of delivery including the following parameters: • origin and shipment details, • reception, reception acknowledgment, • location material/information.
A.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and highlight all non-conformances to this process.
A.DLV_RESP	Procedures shall ensure that people dealing with the procedures for delivery have got the

	required skill, training and knowledge to meet the procedure requirements and to act to be fully in accordance with the above expectations.
A.IC_ORG	Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity of smartcard embedded software and data (e.g. source code and any associated documents) shall exist and be applied in the smartcard IC database construction.
A.USE_TEST	It is assumed that appropriate functionality testing of the smartcard functions is used in phases 3 to 6.
A.USE_PROD	It is assumed that security procedures are used during all manufacturing and test operations through smartcard production phases to maintain the confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
A.USE_SYS	It is assumed that the security of sensitive data stored/handled by the system (terminals, communications ...) is maintained.
A.USE_OPR	after giving a warning message from TSF for corrupted objects (DF-EF-DF PIN-DF PUK, System PIN, System PUK), it is assumed that the user and smart card/terminal application programmer know which corrupted objects can be used or not without taking any risk for security and availability of the TOE.

The information about the phases mentioned above can be found in the Security Target document.

2.4 Architectural Information

Physical scope of TOE covers UKTÜM chip IC UKT23T64H v4, the IC embedded software (UKİS v.1.2.2 OS) and UKİS User Manual. The architectural information about UKT23T64H v4 can be found from its certification report. Operating system consists of Memory Manager, File Manager, Command Interpreter and Communication Handler. Message is received by UART which is managed by communication handler in TOE. The message comes in TPDU (Transmission Protocol Data Unit) format. Incoming TPDU packet is analysed and block type decision is made by the

communication handler. TPDU data is one of 3 different types of block, named R (Receive ready), S (Supervisor) and I (Information) block. R and S blocks are used to control the protocol. I block carries the command which is transmitted to the command interpreter and executed in TOE. When command execution is finished, communication handler sends the answer to the reader via UART. If the command is related with the file system, command interpreter calls the file manager. File manager is responsible for the operations in the file field which is in the NVM. Memory manager is used to open new file, close file, delete page and attach new page.

The operating system consists of 7 subsystem as follows:

1. Cryptographic Operations
2. Cryptographic Keys
3. Authentication and Authorization
4. Secure Messaging
5. Integrity of the Objects
6. Access Conditions on the DFs and EFs
7. Function Countering Physical Attacks

The detailed information about subsystem can be found from the security target and detailed design documents.

2.5 Documentation

Name of Document	Version Number	Publication Date
UKİS (NATIONAL SMART CARD OPERATING SYSTEM) V1.2.2 ON UKT23T64H v4 SECURITY TARGET LITE	21	03.09.2012
Yönetici ve Kullanıcı Kılavuzu(Administrator and User Manual) UKIS v1.2.2 ON UKT23T64H v4	06	08.08.2012

Table 1

2.6 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 which include software, documents, etc 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 UKIS V1.2.2.

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5). There are 29 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 System Test Document according to the TOE Functional Specification documentation.

- **TOE Test Depth:** Developer has prepared TOE System Test Document according to the TOE Design documentation which includes 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 25 sample independent tests. 12 of them are selected from developer`s test plans. The other 13 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- **Penetration Testing:** Evaluator has done 13 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "Sızma Testleri (Penetration Tests)" which is in Annex-C of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

The result of AVA_VAN.5 evaluation is given below:

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

For the TOE, there is no residual vulnerability that they do not affect the evaluation result, found by CCTL (OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

2.7 Evaluated Configuration

Evaluation Evidence: Security Target Document - UKİS (National Smart Card Operating System) versiyon 1.2.2 on UKT23T64H v4 Security Target
Version Number and Date: 20, 07.08.2012

Evaluation Evidence: Security Target Lite Document - UKİS (National Smart Card Operating System) versiyon 1.2.2 on UKT23T64H v4 Security Target Lite
Version Number and Date: 21, 03.09.2012

Evaluation Evidence: Functional Specification Document(UKIS Fonksiyonel Belirtim)
Version Number and Date:06, 15.08.2012

Evaluation Evidence: TOE Design Specification Document(UKIS Ayrıntılı Tasarım Dokümanı)
Version Number and Date:05, 07.08.2012

Evaluation Evidence: Security Architecture Document(UKIS Güvenlik Mimari Dokümanı)
Version Number and Date:08, 07.08.2012

Evaluation Evidence: Administrator and User Manual (UKIS Yönetici Kullanıcı Kılavuzu)
Version Number and Date: 06, 08.08.2012

Evaluation Evidence: TOE Source Code-UKIS V122
Version Number and Date: 01, 05.01.2011

Evaluation Evidence: Development Tools Document-UKİS Gelistirme Ortam Güvenlik Gelistirme Aletleri
Version Number and Date: 04, 22.05.2012

Evaluation Evidence: Preparation Document- UKİS Gelistirme Ortam Güvenlik Gelistirme Aletleri
Version Number and Date: 04, 22.05.2012

Evaluation Evidence: Delivery Document-UKIS Teslim ve İşletim
Version Number and Date: 04, 24.05.2012

Evaluation Evidence: Delivery Document- UKIS Açıklık Analizi Belgesi
Version Number and Date: 04, 17.07.2012

Evaluation Evidence: Configuration Management Document and Configuration List- UKİS Konfigürasyon Yönetim Planı
Version Number and Date: 07, 15.08.2012

Evaluation Evidence: Development Environment Security Document- UKİS Geliştirme Ortam Guvenlik Geliştirme Aletleri
Version Number and Date: 04, 22.05.2012

Evaluation Evidence: TOE Life-Cycle Document- UKIS_KullanimOmru
Version Number and Date: 03, 08.08.2012

Evaluation Evidence: TOE Life-Cycle Document- AKİS UKİS ATR
Version Number and Date: 01, 09.02.2012

Evaluation Evidence: Test Document- UKIS Sisstem Test Dökumanı
Version Number and Date: 04, 08.08.2012

Evaluation Evidence: Test Coverage Analysis Document- UKIS Sisstem Test Dökumanı
Version Number and Date: 04, 08.08.2012

Evaluation Evidence: Test Depth Analysis Document- UKIS Sisstem Test Dökumanı
Version Number and Date: 04, 08.08.2012

Evaluation Evidence: Target of Evaluation (TOE) - UKİS (National Smart Card Operating System) v1.2.2 on UKT23T64H v4
Version Number: 1.2.2

2.8 Results of the Evaluation

Table 2 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with AVA_VAN.5.

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	Derived Security Requirements
ASE_TSS.1	TOE Summary Specification
ASE_COMP.1	Consistency of Security Target
ADV_ARC.1	Security Architecture
ADV_FSP.4	Functional Specification
ADV_IMP.1	Implementation Representation
ADV_TDS.3	TOE Design
ADV_COMP.1	Composite Design Compliance
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Configuration Management Capabilities
ALC_CMS.4	Configuration Management Capabilities
ALC_DEL.1	Delivery
ALC_DVS.1	Development Security
ALC_LCD.1	Life-cycle Definition
ALC_TAT.1	Tools and Techniques
ALC_COMP.1	Integration of Composition Parts and Consistency of Delivery Procedures
ATE_COV.2	Coverage
ATE_DPT.1	Depth
ATE_FUN.1	Functional Tests
ATE_IND.2	Independent Testing
ATE_COMP.1	Composite Functional Testing
AVA_VAN.5	Vulnerability Analysis
AVA_COMP.1	Composite Vulnerability Assesment

Table 2

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 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 UKİS (National Smart Card Operating System) v1.2.2 on UKT23T64H v4 the results of the assessment of all evaluation tasks are “Pass”.

UKİS (NATIONAL SMART CARD OPERATING SYSTEM) v 1.2.2 on UKT23T64H v4 product was found to fulfill the Common Criteria requirements for each of 29 assurance families

and provide the assurance level EAL 4+ (AVA_VAN.5). This result shows that TOE is resistant against the **"HIGH"** 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 that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of UKİS (National Smart Card Operating System) v1.2.2 on UKT23T64H v4 product, result of the evaluation, or the ETR.

3 SECURITY TARGET

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

Name of Document: UKİS (National Smart Card Operating System) version 1.2.2 on UKT23T64H v4 Security Target

Version No.: 20

Date of Document: 07.08.2012

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.

Name of Document: UKİS (National Smart Card Operating System) version 1.2.2 on UKT23T64H v4 Security Target Lite

Version No.: 21

Date of Document: 03.09.2012

4 GLOSSARY

CCCS:	Common Criteria Certification Scheme
CCTL:	Common Criteria Test Laboratory
CCMB:	Common Criteria Management Board
CEM:	Common Evaluation Methodology
AKiS:	Smart Card Operating System (Akıllı Kart İşletim Sistemi)
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

5 BIBLIOGRAPHY

[1]Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2]Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3]Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4]Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3,July 2009

[5] Smartcard Embedded Software Protection Profile, ANSSI-PP-9810, 19th November 1998, Common Criteria for IT Security Evaluation Protection Profile

[6] Machine Readable Travel Document with „ICAO Application", Basic Access Control; BSI-CC-PP-0055, Version 1.10, 25th March 2009, Bundesamt für Sicherheit in der Informationstechnik

[7]PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

[8] Evaluation Technical Report (Document Code: DTR 10 TR 01), v1.0, August 10, 2012

[9] Evaluation Technical Report (Document Code: DTR 10 TR 01), v1.1, August 16, 2012

[10] CC Supporting Document Guidance, Mandatory Technical Document, Composite Product Evaluation for Smartcards and Similar Devices, Version 1.0 Revision 1, September 2007, CCDB-2007-09-001

[11] UKİS (National Smart Card Operating System) version 1.2.2 on UKT23T64H v4 Security Target Version: 20 Date: 07.08.2012

[12] UKİS (National Smart Card Operating System) version 1.2.2 on UKT23T64H v4 Security Target Lite Version:21 Date:03.09.2012

[13] Platform ETR for composite evaluation:

- UKT23T64H v4 Evaluation Technical Report, version1.1, 07.06.2012
- UKT23T64H v4 Test Document, Version 04, 12.03.2012

[14]Platform Data Sheets, Manuals and Guides for Application developer:

- UKTÜM Güvenlik Gerekleri(Security Requirements), Version 01, 11.06.2009
- UKTÜM Güvenlik Önerileri(Security Suggestions), Version 01, 21.09.2010

[15]Platform Security Target and Security Target Lite:

- Security Target Document of Turkish National Smart Card IC UKT23T64H v4 with DES v4.2, AES256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software Version:06, 07.06.2012

- Security Target Lite Document of Turkish National Smart Card IC UKT23T64H v4 with DES v4.2, AES256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software Version:07, 30.06.2012

[16]Delivery and Acceptance Procedure Evidence:

- UKTÜM Üretime Teslim Dokumani(Delivery to Production Document), Version 01, 31.05.2011

[17]Composite Configuration Evidence:

- UKT23T64H v4 TD Teslim Dokumanı(Delivery Document), Version 02, 21.02.2012
- UKTÜM Üretime Teslim Dokumani(Delivery to Production Document), Version 01, 31.05.2011
- AKİS UKİS ATR, Version 01,09.02.2012
- HHNEC Memory Request Form.xls, HFDS-0012-16 (Customer Database MT Information Sheet`09.xls)
- HHNEC Tape out Guide Line For CL250/CM250G7EF250 Processes

6 ANNEXES

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