Certification Report

EAL 4+ (ATE_DPT.2, AVA_VAN.5) Evaluation of

DATAKOM ELEKTRONİK MÜHENDİSLİK A.Ş.

DATAKOM DTC-100 v1.1 VEHICLE UNIT

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: TSE-CCCS-32

TABLE OF CONTENTS

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	**Doküman No**	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	**Yayın Tarihi**	30/07/2015	
		Revizyon Tarihi	25/04/2016	**No** 03

Document Information

Date of Issue	25.04.2016
Version of Report	v1.0
Date Approved	26.04.2016
Certification Report Number	21.0.03/16-001
Sponsor and Developer	DATAKOM ELEKTRONİK MÜHENDİSLİK A.Ş.
Evaluation Lab	TÜBİTAK BİLGEM OKTEM
TOE	DATAKOM DTC-100 v1.1
Pages	18

Author	İbrahim Halil KIRMIZI
Technical Responsible	Zümrüt MÜFTÜOĞLU

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
V1.0	25.04.2016	All	First Release

DISCLAIMER

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

FOREWORD

The Certification Report is drawn up to submit the Certification Commission 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 CSCD (Cyber Security Certification Directorate) Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

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

CCTL (Common Criteria Testing Laboratory) is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM 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 DATAKOM DTC-100 v1.1 whose evaluation was completed on 14.04.2016 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.1. of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the CSCD Certified Products List at 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

Sayfa 5/18

Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.
Basım tarih ve saati: 12.05.2016 11:43

1 - EXECUTIVE SUMMARY

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

Evaluated IT product name: DATAKOM DTC-100

IT Product version: v1.1

Developer's Name: DATAKOM ELEKTRONİK MÜHENDİSLİK A.Ş.

Name of CCTL: TÜBİTAK BİLGEM OKTEM

Assurance Package: EAL 4+ (ATE_DPT.2, AVA_VAN.5)

Completion date of evaluation: 14.04.2015

1.1 Brief Description

The TOE is a vehicle unit (VU) intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards.

The TOE provides the following services;

- Monitoring cards insertions and withdrawals,
- Speed and distance measurement,
- Time measurement,
- Monitoring driver activities,
- Monitoring driver status,
- Driver's manual entries,
- Company locks management,
- Monitoring control activities,
- Detection of events and/or faults,
- Built-in and self-tests,
- Reading from data memory,
- Recording and storing in data memory,

- Reading from tachograph cards,

- Recording and storing in tachograph cards,

- Displaying,

- Printing,

- Warning,

- Data downloading to external media,

- Output data to additional external devices,

- Calibration,

- Time adjustment,

- Software Upgrade

1.2 TOE Security Functions

The TOE has been developed in terms of Appendix [3]. The Security Functions which are compliant to the requirements of Appendix [3] are;

- Identification and Authentication

- Access Control

- Accountability

- Audit

- Object re-use

- Accuracy

- Reliability of Service

- Data Exchange

- Cryptographic Support

- Software Upgrade

1.3 Threats

Threats averted solely by the TOE are;

- **T.Card_Data_Exchange**: Users could try to modify user data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).

- **T.Faults**: Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.

- **T.Output_Data**: Users could try to modify data output (print, display or download).

Threats averted by the TOE and its operational environment are;

- **T.Access**: Users could try to access functions6 not allowed to them (e.g. drivers gaining access to calibration function).

- **T.Calibration_Parameters**: Users could try to use miscalibrated equipment (through calibration data modification, or through organisational weaknesses).

- **T.Clock**: Users could try to modify internal clock.

- **T.Design**: Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery …) or from reverse engineering.

- **T.Environment**: Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).

- **T.Fake_Devices**: Users could try to connect fake devices (motion sensor, smart cards) to the VU.

- **T.Hardware**: Users could try to modify VU hardware.

- **T.Identification**: Users could try to use several identifications or no identification.

- **T.Motion_Data**: Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).

- **T.Power_Supply**: Users could try to defeat the VU security objectives by modifying (cutting, reducing, increasing) its power supply.

- **T.Security_Data**: Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.

- **T.Software**: Users could try to modify VU software on the VU.

- **T.Stored_Data**: Users could try to modify stored data (security or user data).

- **T.Tests**: The use of non-invalidated test modes or of existing back doors could compromise the VU security.

Threat averted solely by the TOE's operational environment is;

- **T.Non_Activated**: Users could use non activated equipment.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-32
TOE Name and Version	DATAKOM DTC-100 v1.1
Security Target Title	DATAKOM DTC-100 v1.1 Vehicle Unit
Security Target Version	V1.1
Security Target Date	12.02.2016
Assurance Level	EAL4+ (ATE_DPT.2, AVA_VAN.5)
Criteria	- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	BSI-CC-PP-0057 Protection Profile 'Digital Tachograph – Vehicle Unit (VU PP)'

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	**Doküman No**	BTBD-03-01-FR-01	
		Yayın Tarihi	30/07/2015	
	CCCS CERTIFICATION REPORT	**Revizyon Tarihi**	25/04/2016	**No** 03

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012, conformant
Sponsor and Developer	DATAKOM ELEKTRONİK MÜHENDİSLİK A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE-CCCS

2.2 Security Policy

Organizational Security Policies related to the TOE are;

- **OSP.Accountability**: The VU must collect accurate accountability data.
- **OSP.Audit:** The VU must audit attempts to undermine system security and should trace them to associated users.
- **OSP.Processing:** The VU must ensure that processing of inputs to derive user data is accurate.
- **OSP.Test_Points:** All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU must be disabled.

Organizational Security Policies related to the TOE and its operational environment are;

- **OSP.Type_Approved_MS:** The VU shall only be operated together with a motion sensor being type approved according to Appendix [3]
- **OSP.Software_Upgrade:** In order to fulfill the software requirements RLB_204, RLB_205 of GST in Appendix [3], the software upgrade process must be carried out in a secure way.

Organizational Security Policies related to the TOE's operational environment are;

- **OSP.PKI:**

o The European Authority shall establish a PKI according to Appendix [3], sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of the PKI.

o The ERCA shall securely generate its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs.

o The ERCA shall ensure that it issues MSi.C certificates only for the rightful MSCAs.

o The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.

o MSCAs shall securely generate their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.

o MSCAs shall ensure that they issue EQTj.C certificates only for the rightful equipment.

- **OSP.MS_Keys:**

  o The European Authority shall establish a special key infrastructure for management of the motion sensor keys according to Appendix [5] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure.

  o The ERCA shall securely generate both parts (KmVU and KmWC) of the master key (Km).

  o The ERCA shall ensure that it securely convey this key material only to the rightful MSCAs.

  o The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.

  o MSCAs shall securely calculate the motion sensor identification key (KID) and the motion sensor's credentials: MS individual serial number encrypted with the identification key (Enc(KID|NS)) and MS individual pairing key encrypted with the master key (Enc(KM|KP)).

  o MSCAs shall ensure that they issue these MS credentials , KmVU and KmWC only to the rightful equipment.

2.3 Assumptions and Clarification of Scope

- **A.Activation**: Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.

- **A.Approved_Workshops**: The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.

- **A.Card_Availability**: Tachograph cards are available to the TOE users and delivered by Member State authorities to authorised persons only.

- **A.Card_Traceability**: Card delivery is traceable (white lists, black lists), and black lists are used during security audits.

- **A.Controls**: Law enforcement controls will be performed regularly and randomly, and must include security audits (as well as visual inspection of the equipment).

- **A.Driver_Card_Uniqueness**: Drivers possess, at one time, one valid driver card only.

- **A.Faithful_Calibration**: Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.

- **A.Faithful_Drivers**: Drivers play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected …).

- **A.Regular_Inspections**: Recording equipment will be periodically inspected and calibrated.

2.4 Architectural Information

TOE is a device to be installed in a vehicle. The TOE consists of a hardware box (includes a processing unit, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration/downloading connector, facilities for entry of user's inputs, embedded software and of related user manuals. It must be connected to a motion sensor (MS) and to a power supply unit; it can temporarily be connected with other devices used for calibration, data export and diagnostics.

2.5 Documentation

During the evaluation; the configuration of evaluation evidences which also include Source Code, Common Criteria related documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Publication Date
DATAKOM DTC-100 Vehicle Unit	1.1	22.02.2016
cryptoDevice.sln	v.1990	

DATAKOM DTC-100 v1.1 Vehicle Unit Security Target	1.1	12.02.2016
DATAKOM DTC-100 Functional Specification	1.5	25.01.2016
DATAKOM DTC-100 Design Description	1.10	11.04.2016
DATAKOM DTC-100 Architecture Description	1.4	13.11.2015
DATAKOM DTC-100 Installation	0.1	08.03.2014
DATAKOM DTC-100 User Manual	0.4	20.10.2014
DATAKOM DTC-100 Development Security Documentation	0.5	10.11.2014
DATAKOM DTC-100 Delivery Procedure	0.2	23.09.2014
DATAKOM DTC-100 Configuration Management	0.5	30.11.2015
DATAKOM DTC-100 Life Cycle Definition	0.4	22.05.2015
DATAKOM DTC-100 Test Analysis Document	0.8	10.12.2015

Table 1 - Documentation

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 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 final Evaluation Technical Report (ETR) of DATAKOM DTC-100 v1.1.

It is concluded that the TOE supports EAL 4+ (ATE_DPT.2, AVA_VAN.5). There are 24 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

2.6.1 Developer Testing:

- TOE Test Coverage: Developer has prepared TOE Test Analysis Document according to the TOE Functional Specification documentation.
- TOE Test Depth: Developer has prepared TOE Test Analysis 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.

2.6.2 Evaluator Testing:

The tests were performed with the product DATAKOM DTC-100 v1.1.

- Independent Testing: Evaluator has done a total of 21 sample independent tests. 11 of them are selected from developer`s test plans. The other 10 tests are evaluator`s independent tests. All of them are related to TOE security functions.

- Penetration Testing: Evaluator has done 10 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "TOE Security Functions Penetration Tests Scope" which is in Annex-B of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

- TOE itself,
- Motion Sensor of which interface to Vehicle Unit is conformant to ISO 16844-3:2004 standard.
- Data Download Connector which communicate according to the ISO 14230-2 standard.
- CANBUS

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 ATE_DPT.2 and AVA_VAN.5

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete Functional Specification
	ADV_IMP.1	Implementation Representation of the TSF
	ADV_TDS.3	Basic Modular Design
	AGD_OPE.1	Operational User Guidance

Guidance Documents	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and Automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-defined Development Tools
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.2	Testing: Security Enforcing Modules
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.5	Advanced Methodological Vulnerability Analysis

Table 2 – Security Assurance Requirements of TOE

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 "DATAKOM DTC-100 v1.1" the results of the assessment of all evaluation tasks are "Pass".

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.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "DATAKOM DTC-100 v1.1" product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: DATAKOM DTC-100 v1.1 Vehicle Unit Security Target

Version: 1.1

Date of Document: 12.02.2016

A public version has been created and verified according to ST-Santizing:

Title: DATAKOM DTC-100 v1.1 Vehicle Unit Security Target Lite

Version: 1.2

Date of Document: 02.03.2016

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.

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory (OKTEM)

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

OKTEM : Ortak Kriterler Test Merkezi

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

SSCD: Secure Signature Creation Device

ST : Security Target

STCD :Software Test and Certification Department

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] Annex 1B of Commission Regulation (EEC) No. 1360/2002

[4] BTBD-01-01-TL-01 Certification Report Preparation Instructions, Rel.Date: 08.02.2016

[5] ISO 16844-3:2004 with Technical Corrigendum 1:2006, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface

[6] DTR 51 TR 02 - DATAKOM DTC-100 v1.1 Evaluation Technical Report v0.2

6 ANNEXES

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