REF: 2012-32-INF-2355 v1	Created by: CERT10
Target: Público	Revised by: CALIDAD
Date: 09.05.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2012-32 Aselsan STC-8250A v1.1

Applicant: 0860042250 Aselsan A.S.

References:

[EXT-1930] Certification request of Aselsan STC-8250A v1.1

[EXT-3787] Evaluation Technical Report of Aselsan STC-8250A v1.1.

The product documentation referenced in the above documents.

Certification report of the product Aselsan STC-8250A v1.1, as requested in [EXT-1930] dated 19/10/2012, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3787] received on 28/02/2018.

TABLE OF CONTENTS

EXECUTIVE SUMMARY.

This document constitutes the Certification Report for the certification dossier of the product Aselsan STC-8250A v1.1, a digital tachograph which purpose is record, store, display, print and output data related to driver activities

Developer/manufacturer: Aselsan A.Ş.

Sponsor: Aselsan A.Ş.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: Protection Profile Digital Tachograph-Vehicle Unit (VU-PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik.

Evaluation Level: EAL4 + ATE_DPT.2, AVA_VAN.5.

Evaluation end date: 28/02/2018.

All the assurance components required by the evaluation level EAL4 (augmented with ATE_DPT.2 and AVA_VAN.5) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+, as defined by the Common Criteria for Information Technology Security Evaluation version 3.1 R4 and the Common Methodology for Information Technology Security Evaluation version 3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Aselsan STC-8250A v1.1, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation (TOE) is a vehicle unit (VU) in the sense of Annex I B of Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’ dated 05.08.2002 and amended by Commission Regulation (EC) No 432/2004 of 5 March 2004 Council Regulation (EC) No 1791/2006 of 20 November 2006, Commission Regulation (EC) No 68/2009 of 23 January 2009 and Commission Regulation (EU) No 1266/2009 of 16 December 2009.

The TOE is 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 receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all these user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces.

The block diagram of the TOE is depicted in Figure 1 (it is noted that although the printer mechanism is part of the TOE, the paper document once produced is not).

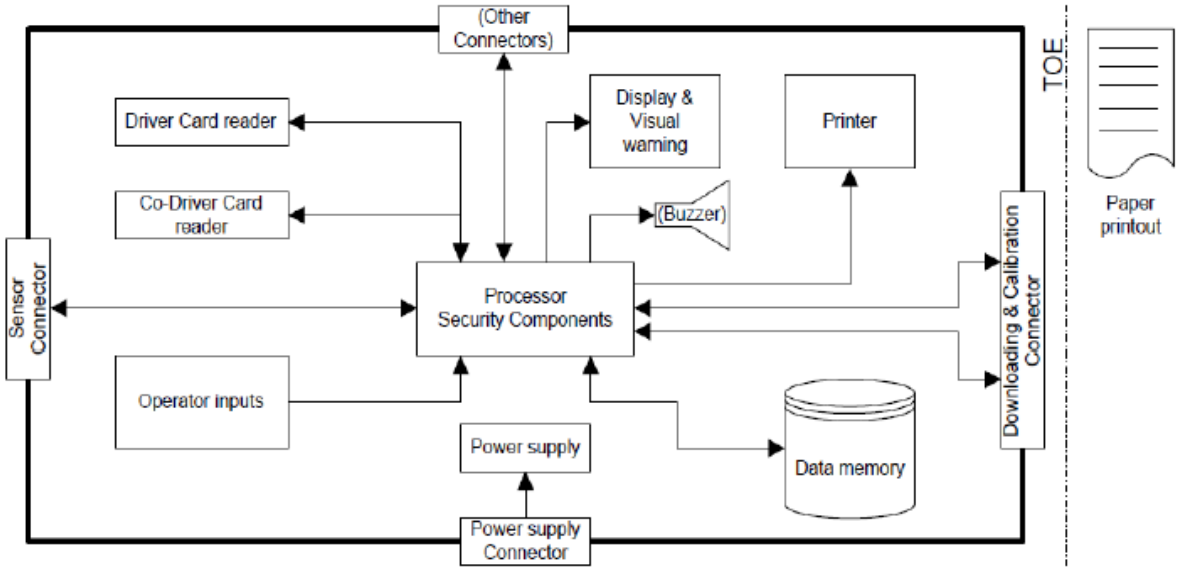

Figure 1: Block Diagram of the TOE

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional components ATE_DPT.2 and AVA_VAN.5, according to Common Criteria v3.1 R4.

Class	Family/Component
ASE: 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
ADV: 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: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.4 Production support, acceptance procedures and

	automation ALC_CMS.4 Problem tracking CM coverage ALC_DVS.1 Identification of security measures ALC_TAT.1 Well-defined development tools ALC_DEL.1 Delivery procedures ALC_LCD.1 Developer defined life-cycle model
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.2 Testing: security enforcing modules ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Component
FAU: Security audit	GEN.1 Audit data generation SAR.1 Audit review STG.1 Protected audit trail storage
FCO: Communication	NRO.1 Selective proof of origin
FCS: Cryptographic Support	CKM.1/TDES Cryptographic key generation CKM.1/AES Cryptographic key generation CKM.2 Cryptographic key distribution CKM.3 Cryptographic key access CKM.4 Cryptographic key destruction COP.1/TDES Cryptographic operation COP.1/RSA Cryptographic operation COP.1/AES Cryptographic operation COP.1/ECDSA Cryptographic operation
FDP: User data protection	ACC.1/FIL Subset access control ACC.1/FUN Subset access control ACC.1/DAT Subset access control ACC.1/UDE Subset access control ACC.1/IS Subset access control ACC.1/SW-Upgrade Subset access control ACF.1/FIL Security attribute based access control ACF.1/FUN Security attribute based access control ACF.1/DAT Security attribute based access control ACF.1/UDE Security attribute based access control ACF.1/IS Security attribute based access control ACF.1/SW-Upgrade Security attribute based access control ETC.2 Export of user data with security attributes ITC.1 Import of user data without security attributes ITC.2//IS Import of user data with security attributes ITC.2//SW-Upgrade Import of user data with security attributes RIP.1 Subset residual information protection SDI.2 Stored data integrity
FIA: Identification and authentication	AFL.1/MS Authentication failure handling

	AFL.1/TC Authentication failure handling ATD.1//TC User attribute definition UAU.1/TC Timing of authentication UAU.1/PIN Timing of authentication UAU.1/MD Timing of authentication UAU.2//MS User authentication before any action UAU.3/MS Unforgeable authentication UAU.3/TC Unforgeable authentication UAU.3/MD Unforgeable authentication UAU.5//TC Multiple authentication mechanisms UAU.6/MS Re-authenticating UAU.6/TC Re-authenticating UID.2/MS User identification before any action UID.2/TC User identification before any action UID.2/MD User identification before any action
FMT: Security management	MSA.1 Management of security attributes MSA.3/FUN Static attribute initialisation MSA.3/FIL Static attribute initialisation MSA.3/DAT Static attribute initialisation MSA.3/UDE Static attribute initialisation MSA.3/IS Static attribute initialisation MSA.3/SW-Upgrade Static attribute initialisation MOF.1 Management of security functions behaviour SMF.1 Specification of Management Functions SMR.1//TC Security roles
FPR: Privacy	UNO.1 Unobservability
FPT: Protection of the TSF	FLS.1 Failure with preservation of secure state PHP.2//Power_Deviation Notification of physical attack PHP.2//HW_sabotage Notification of physical attack PHP.3 Resistance to physical attack STM.1 Reliable time stamps TDC.1//IS Inter-TSF basic TSF data consistency TDC.1/SW-Upgrade Inter-TSF basic TSF data consistency TST.1 TSF testing
FRU: Resource Utilization	PRS.1 Limited priority of service

IDENTIFICATION

Product: Aselsan STC-8250A v1.1 (more details in Table 1)

Security Target: Aselsan STC-8250A Security Target v2.5, 18.10.2017.

Protection Profile: Protection Profile Digital Tachograph-Vehicle Unit (VU-PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010, Bundesamt für Sicherheit in der Informationstechnik.

Evaluation Level: Common Criteria v.3.1 R4 - EAL4 + ATE_DPT.2, AVA_VAN.5.

TOE Identification	Aselsan STC-8250A
TOE Version	v1.1
TOE SW Version	0.8.3
OMAP SW file	name avu-omap-0_8_3_0dpl-0_0_102_signed
ARM SW file name	avu-arm-0_8_3_0dpl-svn2746-20171018
DSP SW file name	AVU_DSP_0_0_102
MSP SP SW file name	avu-msp-0_0_195_63_rls
MSP PP SW Version	avu-msp_pp-0_5_0
TOE HW Version	5820-8250-0001S_RevA
Base Card (TBK)	5999-9945-9002S_RevA
Processor Card (MPK_PRD)	5999-9945-9001_RevB
Processor Card Covers(CR TOP)	5999-0045-9004_RevB
Processor Card Covers(CR BOTTOM)	5999-0045-9005_RevB
Processor Frame Top (FRMT)	5999-0045-9006_RevB
Processor Card Frame Bottom (FRMB)	5999-0045-9007_RevB
Front Panel Card (OPK)	5999-9945-9003S_RevA
Mechanics (MEC)	6009-0045-9006_RevB (Front cover) 5999-9045-9008_RevB (Bottom cover) 5999-9045-9009_RevB (Top cover)

Table 1

SECURITY POLICIES

The use of the product Aselsan STC-8250A v1.1 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 4.5.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 4.6.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Aselsan STC-8250A v1.1, although the agents implementing attacks have the attack potential according to the HIGH of EAL 4 + AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The detail of these threats is documented in the Security Target, section 4.4.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The detail of these security objectives for the TOE operational environment is documented in the Security Target, section 5.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

The section 2.3.2 Logical Scope of the Security Target describes the main security functionality implemented by the TOE:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification & Authentication of Motion Sensor and Tachograph Cards
- Security Management
- Protection of the TSF
- Communication
- Privacy
- Resource utilization

PHYSICAL ARCHITECTURE

The physical scope of the TOE is Aselsan Digital Tachograph Vehicle Unit (Aselsan STC-8250A v1.1) which 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 manuals.

More details can be found in section 2.3.1 of the Security Target.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

The following guides are required reading and part of the TOE:

- **Quick User Guide**. (AVU-QUI-RevA with stamp.pdf)
- **Preparation Manual**. AVU-AGD-PRE, Rev 0.8, 19.10.2017. (AVU-AGD-PRE_v0.8.pdf)
- **Operation Manual**. AVU-AGD-OPE, Rev 0.7, 19.10.2017. (AVU-AGD-OPE-v0.7.pdf)

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated all the developer functional tests in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a test for each of the security functions of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation, in respect to the expected results, was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The evaluator has performed an installation and configuration of the TOE using the information provided in the preparation manual and the operational manual.

The evaluator has followed the security measures described both in preparation manual and the operational manual in order to fulfil the security objectives for the operational environment described in the security target.

The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target.

The following software version has been used:

- MSP SW v 0.195.63 (filename: avu-msp_0_0_195_63_rls.txt).

- OMAP SW v 0.8.3 Deployment version (filename: avu-omap-0_8_3dpl-0_0_102_signed.bin), composed by:
  - DSP SW v. 0.0.102 (filename: AVU_DSP_0_0_102.out).
  - ARM SW v. 0.8.3 Deployment version (filename: avuarm-0_8_3dpl-svn2746-20171018.out).
- Personalization file (filename: keyVAluesVU4_signed.bin).

In addition to this, a production version of OMAP software has been used for specific testing purpose (composed by the same DSP SW version and ARM SW v0.8.3 Production version).

EVALUATION RESULTS

The product Aselsan STC-8250A v1.1 has been evaluated against the Security Target "Aselsan STC-8250A Security Target v2.5, 18.10.2017".

All the assurance components required by the evaluation level EAL4 + ATE_DPT.2, AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the **"PASS" VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ATE_DPT.2, AVA_VAN.5, as defined by Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended as there are not exploitable vulnerabilities for the TOE under its operational environment.

The following usage recommendations are given:

- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Aselsan STC-8250A v1.1, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level

ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Aselsan STC-8250A Security Target. Version 2.5. 18.10.2017.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Aselsan Digital Tachograph Vehicle Unit (v1.1) Security Target (Lite Version). Version 2.6. 26/04/2018.

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.

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 SOGIS 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 "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at *https://www.sogis.org*.

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

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

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), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC 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-2014 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.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.