Scheme Note

Decision Date	Matter ID
2015-09-17	None (Management decision)
Decision by (Name/Title)	Scheme Note Number
Mats Engquist, Quality Manager	20
Presentation by	Present at the Meeting
Dag Ströman, Head of CSEC Martin Bergling, Technical Manager	CCB 2015-09-17

Schematolkningens innebörd/Scheme Note Statement

Description and References

Purpose

This scheme note provides instructions for evaluations of digital tachograph sensors in accordance with COUNCIL REGULATION (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport, Annex 1 B, together with relevant amendments (hereby referred to as "the Regulation").

Introduction

The digital tachograph is a control device for recording drivers' activities, such as driving and rest periods. The digital tachograph is required by law in the European Union as a result of the COUNCIL REGULATION (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport. The EU-ministers have formulated four main topics to be addressed by the introduction of the digital tachograph.

The digital tachograph:

- allows effective and efficient enforcement of drivers' activities,
- gives transport companies more possibilities to use the equipment as management tool,
- provides the drivers with clear and accurate information about their driving and rest periods,
- reduces fraud possibilities.

The reduction of fraud, in combination with improved possibilities for enforcement, is the main reasons for the security of the digital tachograph system. The Regulation formulates security requirements for the following components of the digital tachograph system:

- the motion sensor,
- the vehicle unit, and
- the tachograph cards.

Every manufacturer of these components should demonstrate that the security requirements defined in the Regulation are fulfilled. To do so, a formal security evaluation is required.

General Information

The security requirements for the tachograph components are defined in Annex 1B,

appendix 10 of the Regulation. The Regulation expresses security requirements based on the ITSEC standard for the motion sensor and the vehicle unit. For requirements on the tachograph card, the Regulation refers to two protection profiles [ISPP, ESPP] based on the standard ISO/IEC 15408 (a k a "Common Criteria" - CC).

Since the Regulation was issued, the CC has to most extent replaced the use of the ITSEC standard to express the requirements on the digital tachograph components. In "Security Evaluation and Certification of Digital Tachographs" [JIL 1] the ITSEC certification bodies being signatories of the "Mutual Recognition Agreement of Information Technology Security Evaluation" (SOG-IS MRA) have issued a joint interpretation describing how the ITSEC based requirements of the Regulation may be expressed according to the CC. This scheme note is written in accordance with this interpretation.

Certificates of CC evaluations of tachograph sensors issued by FMV/CSEC will be subject for mutual recognition within the following arrangements and associated claims of conformance:

- EAL4 augmented with DPT.2 and VAN.5 within EA-MLA.
- EAL4 within SOG-IS MRA.
- EAL2 within CCRA.

Charges and fees for a certification of a sensor will be in accordance with the scheme publication SP-008 “Charges and Fees” and consist of:

- Application fee.
- Certification fee for product with complexity class A, EAL4.
- A charge of 80 hours covering the extra certifciation cost of the augmentations of EAL4 with ATE_DPT.2 and AVA_VAN.5.
- A charge of 16 hours covering the extra cost for verification that the security target covers the requirements specified in the Regulation.

More background information about the digital tachograph can be found in the Regulation, the "European digital tachograph common security guideline" [SECGUIDE], and "Impact assessment on measures enhancing the effectiveness and efficiency of the tachograph system Revision of Council Regulation (EEC) No 3821/85" [SEC(2011) 948 final].

Requirements

The evaluator shall verify that the security target (at least) claim the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, corresponding to E3hAP described in "Security Evaluation and Certification of Digital Tachographs" [JIL 1].

The evaluator shall provide a written analysis that demonstrates that the security target of the sensor to be evaluated fulfils the minimum requirements that are laid out in the Regulation. This analysis shall demonstrate:

- that the security functional requirements of the sensor specified in the Regulation is covered by the security target for the sensor to be evaluated, and
- that sensor requirements not covered by the target of evaluation (TOE) is listed as requirements on the environment of the TOE.

The evaluator shall apply relevant parts of “Security Evaluation and Certification of Digital Tachograph’s” [JIL 1].

For calculation of the attack potential of attacks that shall be included in the vulnerability analysis, the evaluator shall apply relevant parts of the SOG-IS MRA supporting document “Application of Attack Potential to Hardware Devices with Security Boxes”

[JIL 2].

The evaluator shall provide a written statement to FMV/CSEC that demonstrates that the evaluators have the necessary competence and experience to perform the vulnerability analysis of tachograph sensors according to the Regulation.

In case the vulnerability analysis shows that penetration testing is necessary, the evaluator shall provide a written statement to FMV/CSEC that demonstrates that the ITSEF has access to necessary staff with adequate competence, experience, time and equipment to perform such penetration tests.

Since the cryptographic standards used by the tachograph sensor are prescribed in the Regulation, the evaluator shall not include the cryptographic strength of cryptographic algorithms, schemes and protocols specified in the Regulation during the vulnerability analysis. In the final evaluation report the evaluator shall include a statement that above exception has been made. However, correct implementation of such cryptographic standards is to be included in the evaluation and associated vulnerability analysis.

In addition to this scheme note, the evaluator shall apply the following scheme notes:

- Scheme Note 11 - Methodology for AVA_VAN 4 and 5 [SN11]
- Scheme Note 15 - Demonstration of test coverage [SN15]
- Scheme Note 16 - Additional planning requirements [SN16]
- Scheme Note 18 - Highlighted Requirements on the Security Target [SN18]

References

EU 3821/85	COUNCIL REGULATION (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport, Annex 1 B
EU 1161/2014	Commission Regulation (EU) No 1161/2014 of 30 October 2014 adapting to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport
ICPP	Smartcard Integrated Circuit Protection Profile — version 2.0 — issue September 1998. Registered at French certification body under the number PP/9806
ESPP	Smart Card Integrated Circuit With Embedded Software Protection Profile version 2.0 issue June 99. Registered at French certification body under the number PP/9911
SECGUIDE	European digital tachograph common security guideline, version 1.0, 5 November 2002
SEC(2011) 948 final	Commission Staff Working Paper - Impact assessment on measures enhancing the effectiveness and efficiency of the tachograph system Revision of Council Regulation (EEC) No 3821/85, Brussels, 19.7.2011
JIL 1	Security Evaluation and Certification of Digital Tachographs, Version 1.12, June 2003
JIL 2	Application of Attack Potential to Hardware Devices with Security Boxes, version 1.0, May 2012
SN11	Scheme note 11 - "Methodology for AVA_VAN 4 and 5"
SN15	Scheme Note 15 - "Demonstration of test coverage"

SN16	Scheme Note 16 - "Additional planning requirements"
SN18	Scheme Note 18 - "Highlighted Requirements on the Security Target"
SOG-IS MRA	Mutual Recognition Agreement of Information Technology Security Evaluation version 3.0, 8 January 2010
TSFS 2013:1	Transportstyrelsens föreskrifter om hantering av krypteringsnycklar och certifikat för tillverkning av digitala färdskrivare
TSFS 2013:3	Transportstyrelsens föreskrifter om ackreditering av kontrollorgan, kontroll och plombering av färdskrivare samt installationsskylt