EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

Digital Tachograph Motion Sensor Protection Profile Clarifications

Version 1, February 2025

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
September 2024	V0.1	Creation	Based on JIL Tachograph MS PP Clarification
February 2025	V1	Update based on EUCC maintenance subgroup comments	Endorsed for publication on 11/03/2025 by the ECCG

LEGAL NOTICE

DISCLAIMER

This draft version of the state-of-the-art document is published for information only. Following endorsement by the ECCG, it was submitted for inclusion in the list of applicable state-of-the-art documents listed in Annex I of Commission Implementing Regulation (EU) 2024/482.

It received a positive opinion from the ECCG but has not yet been adopted by the Commission via an amendment of the Implementing Regulation (EU) 2024/482. State-of-the-art documents will only become applicable and legally binding following their inclusion in the Implementing Regulation and in line with relevant transition rules specified by such regulation.

Therefore, this document should not yet be considered as final and legally binding. Furthermore, changes might be introduced in state-of-the-art documents in the context of the comitology procedure.

LEGAL NOTICE

This publication is a state-of-the-art document as defined in Article 2 point 14 of Commission Implementing Regulation (EU) 2024/482.

This document is established and endorsed by the European Cybersecurity Certification Group (ECCG) in accordance with Article 48 paragraphs 2 and 3 of Commission Implementing Regulation (EU) 2024/482.

This document shall be updated whenever needed to reflect the developments and best practices in the field of the evaluation of digital tachographs. Updates of this document shall be submitted to the ECCG for endorsement.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

This state-of-the-art document as defined under Article 2 point 14 of Regulation (EU) 2024/482 is a supporting document under Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC).

It provides clarifications of the Common Criteria Protection Profile Digital Tachograph - Motion Sensor (MS PP)[1], Version 1.0, 9 May 2017.

The MS PP is referred to in Annex III of the EUCC scheme and is intended to specify the Common Criteria IT security requirements for a motion sensor of a digital tachograph system in order to cover the IT security requirements of Regulation (EU) 165/2014, as specified in Commission Implementing Regulation (EU) 2016/799 (Annex 1C).

The objective of these clarifications is to allow a harmonised application of the MS PP in order to fulfill the IT-security requirements of Regulation (EU) 165/2014, as specified in Commission Implementing Regulation (EU) 2016/799 (Annex 1C).

1.2 NORMATIVE REFERENCES

Regulations

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)[2], as amended by Implementing Regulation 2024/3144.

Standards

Note: Unless otherwise specified, the versions of the Common Criteria and Common Evaluation Methodology standards defined in Article 2 of the EUCC scheme apply.

EUCC state-of-the-art documents[3]

Note: Unless otherwise specified, the latest version of referenced state-of-the-art documents applies.

1.3 ACRONYMS

CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
CSA	Cybersecurity Act
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EU	European Union
ICT	Information and communications technology

[1] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0093b_pdf.pdf
[2] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj
[3] Available at https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

IT	Information technology
ITSEF	Information Technology Security Evaluation Facility
ST	Security target
TOE	Target of evaluation
TS	Technical specification
TSFI	TOE security function interfaces

2. CLARIFICATIONS

The MS PP includes amongst others the following non-hierarchical Security Functional Requirements (SFRs):

- FPT_PHP.2 Notification of physical attack (with application note 8[4]);
- FPT_PHP.3 Resistance to physical attack (iteration 1[5] and 2[6]).

FPT_PHP.2 requires opening detection with (active) notification as well as passive detection; application note 8 clarifies that opening detection with (active) notification is only required in the case that the target of evaluation (TOE) can be opened.

FPT_PHP.3 Resistance to physical attack (iteration 1 and 2) has to be fulfilled by the TOE in any case.

This means that:

- In any case the TOE shall resist to physical tampering attacks to the TOE security functionality (TSF) software and TSF data, and provide unambiguous detection of physical tampering that might compromise the TSF.
- In the case that the TOE is equipped with an opening mechanism (e.g.: a screw top), the TOE shall in addition:
    - provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred and;
    - monitor the devices and elements and notify [a paired Vehicle Unit] when physical tampering with the TSF's devices or TSF's elements has occurred.

[4] If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of 6 months. It is acceptable that the audit record is stored after power supply reconnection. If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g.: through visual inspection), and FPT_PHP.2.3 is not relevant (penetration of the case by other means is addressed by FPT_PHP.2.2)..
[5] The TSF shall resist [use of magnetic fields to disturb vehicle motion detection] to the [TOE components implementing the TSF] by responding automatically such that the SFRs are always enforced.
[6] The TSF shall resist [physical tampering attacks] to the [TSF software and TSF data] by responding automatically such that the SFRs are always enforced.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu