SLOVENSKI STANDARD
SIST EN 50436-6:2015

01-september-2015

Alkoholne zapore - Preskusne metode in zahtevane lastnosti - 6. del: Varnost podatkov

Alcohol interlocks - Test methods and performance requirements - Part 6: Data security

Alkohol-Interlocks - Prüfverfahren und Anforderungen an das Betriebsverhalten - Teil 6: Datensicherheit

Ethylotests anti-démarrage - Méthodes d'essai et exigences de performance - Partie 6: Sécurité des données

Ta slovenski standard je istoveten z: **EN 50436-6:2015**

ICS:

43.040.10	Električna in elektronska oprema	Electrical and electronic equipment
71.040.40	Kemijska analiza	Chemical analysis

SIST EN 50436-6:2015 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50436-6

March 2015

ICS 43.040.10; 71.040.40

English Version

Alcohol interlocks - Test methods and performance requirements - Part 6: Data security

Éthylotests antidémarrage - Méthodes d'essai et exigences de performance - Partie 6: Sécurité des données

Alkohol-Interlocks - Prüfverfahren und Anforderungen an das Betriebsverhalten - Teil 6: Datensicherheit

This European Standard was approved by CENELEC on 2014-12-29. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (EN 50436-6:2015) has been prepared by CLC/BTTF 116-2 "Alcohol interlocks".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-12-29
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2017-12-29

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Introduction

The series of European Standards EN 50436 specifies test methods and essential performance requirements for alcohol interlocks and gives guidance for decision makers, purchasers and users. The content and requirements of the European Standard EN 50436-1 "Alcohol interlocks – Test methods and performance requirements, Part 1: Instruments for drink-driving-offender programs" are based on the experience and necessities of drink driving offender programmes in different countries over several decades.

The present document should be used in conjunction with the European Standard EN 50436-1 and optionally with EN 50436-2. It defines additional requirements for the security of event records which are stored in the data memory of the alcohol interlock and which may be downloaded, processed and transferred to supervising persons or organizations.

The security objectives describing how the threats are addressed are divided into security objectives for the alcohol interlock with the service application and for the operational environment.

The security objectives for the alcohol interlock and the service application describe what is necessary for the alcohol interlock and the service application to do to address the threats. In the context of this European Standard, the combination of alcohol interlock and service application are to meet all listed security objectives, and this is to be assessed as part of determining compliance with this European Standard.

The security objectives for the operational environment describe what other entities should do to address the threats. In the context of this European Standard, whether these entities actually achieve these objectives are not to be assessed as part of determining compliance with this European Standard. Therefore, in this European Standard these security objectives are informative only.

This European Standard is intended also to be listed as a Protection Profile for alcohol interlocks under the Common Criteria Recognition Arrangement and the Senior Officials Group - Information Systems Security (SOG-IS). For the purpose of being a Protection Profile, all sections (including also the operational environment) are considered normative.

1 Scope

1.1 General

This European Standard specifies security requirements for the protection and handling of event records which are stored in the data memory of breath alcohol controlled alcohol interlocks and which may be downloaded, processed and transferred to supervising persons or organizations.

This European Standard is a supplement to EN 50436-1. It is to be decided by the respective jurisdiction whether the present standard has to be applied in addition to EN 50436-1.

This European standard may also be used as a supplement to EN 50436-2 if a jurisdiction or a vehicle fleet operator decides that the data security in his preventive application has to have the same high level of requirements as for alcohol interlocks used in drink-driving-offender programmes.

This European Standard is mainly directed to test houses, manufacturers of alcohol interlocks, legislating authorities and organizations which handle and use the alcohol interlock event records.

In this European Standard, the alcohol interlock consists basically of handset and control unit. Optional accessory devices (e.g. cameras or GPS systems generating data related to event data of the alcohol interlock, as well as accessory devices handling or transferring data for a drink-driving-offender programme) authorized by the manufacturer as being part of the alcohol interlock system and which are intended to be used in the vehicle during operation are also to be considered part of the alcohol interlock, where applicable.

The service application communicates with the alcohol interlock and sends out the event records to a register, either directly or alternatively indirectly through a broker.

The scheme is depicted in Figure 1. It also shows which parts are within the scope of this European Standard and which are outside of the scope.

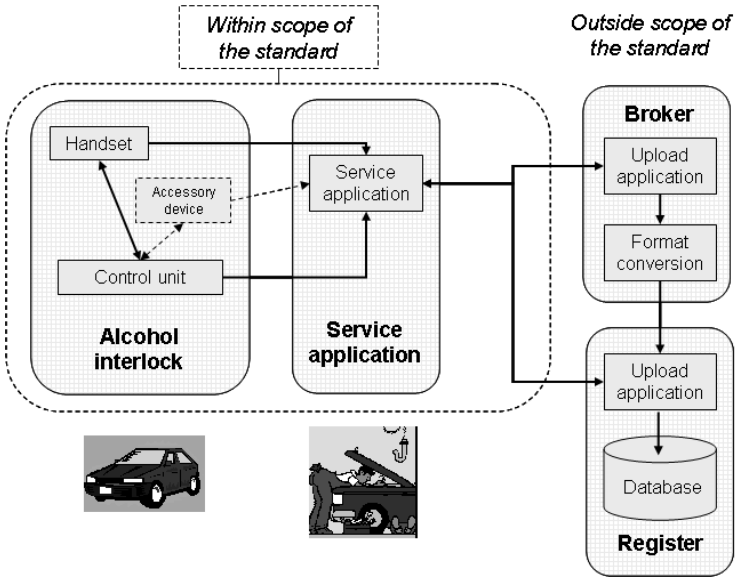

Figure 1 – Alcohol interlock, service application, broker and register

NOTE In this, and all other figures, the direction of the arrows indicates the flow of event records.

This European Standard applies to

– the alcohol interlock,

– the service application.

This European Standard does not apply to

– data security of the broker,

– data security of the register,

– storage of downloaded data,

– requirements for organizational processes, for example defining rights of access to the data.

1.2 Conformance claim

This European Standard conforms according to the Common Criteria for Information Technology Security Evaluation as Protection Profile to:

– Common Criteria, Version 3.1, Revision 4, as defined by CCp1, CCp2, CCp3 and CEMe,

– Common Criteria - Part 2 as Common Criteria - Part 2 conformant,

– Common Criteria - Part 3 as Common Criteria - Part 3 conformant.

NOTE 1 An earlier revision of CCp1 is published as ISO/IEC 15408-1.

NOTE 2 An earlier revision of CCp2 is published as ISO/IEC 15408-2.

NOTE 3 An earlier revision of CCp3 is published as ISO/IEC 15408-3.

NOTE 4 An earlier revision of CEMe is published as ISO/IEC 18045.

This European Standard is not based on any other Protection Profile.

This European Standard conforms to the evaluation assurance level EAL3 + ALC_FLR.2 (for explanation see 7.4).

Protection profiles or security targets that conform to this Protection Profile shall apply "Strict Protection-Profile-Conformance".

For more information, see CCp1, Annex B5.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50436-1:2014, *Alcohol interlocks – Test methods and performance requirements – Part 1: Instruments for drink-driving-offender programs*

EN 50436-2:2014, *Alcohol interlocks – Test methods and performance requirements – Part 2: Instruments having a mouthpiece and measuring breath alcohol for general preventive use*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
alcohol interlock
device which is normally in the blocking state when installed to prevent the starting of a vehicle engine, and which can be brought into the not-blocking state only after the presentation and analysis of an accepted breath sample with an alcohol concentration below a limit value

Note 1 to entry: In this European Standard the expression “starting of the vehicle engine” includes provision of an output signal from the alcohol interlock to the vehicle to enable the starting or operation of the vehicle.

Note 2 to entry: In this European Standard, the alcohol interlock consists of the following parts: handset, control unit and optional accessory devices.

Note 3 to entry: According to the Common Criteria the alcohol interlock and the service application are the Target of Evaluation (TOE).

3.2
handset
part of the alcohol interlock which is usually located inside the driver compartment of the vehicle, which contains an alcohol measuring system, may store event records in a data memory, is connected to the control unit and is able to interact with the driver

3.3
control unit
part of the alcohol interlock which is usually located under the dashboard of the vehicle, which is electrically connected to the vehicle to prevent or to allow the starting of the vehicle engine, and which may store event records in a data memory

Note 1 to entry: The electrical connections to the vehicle are considered to be part of the control unit.

3.4
accessory device
optional supplementary device being part of the alcohol interlock intended to be used in the vehicle during operation

Note 1 to entry: Accessory devices may for example be a camera or a module for data transmission.

Note 2 to entry: The use of certain accessory devices may be required by national regulations.

3.5
event records
record of breath test results, other events and supporting data with date and time generated by the alcohol interlock

Note 1 to entry: For this European Standard it is assumed that the event records are stored in the data memory of the control unit and/or of the handset and optionally of the accessory devices.

Note 2 to entry: This European Standard uses the term “event records" instead of the Common Criteria term “audit records”.

3.6
service application
computer programme being used for functions such as adjustment of the alcohol interlock, downloading and optionally viewing the event records and other data of the alcohol interlock, as well as for uploading event records from the alcohol interlock to a register or broker

Note 1 to entry: A service application may have some or all of these functions, depending on its implementation and the alcohol interlock class (see Clause 5).

Note 2 to entry: The service application is usually located inside a service centre.

Note 3 to entry: The service application may be used by a technician or an automatic system.

Note 4 to entry: The service application may be either transparent or opaque.

3.7
transparent service application
service application which is not able to decrypt the event records

Note 1 to entry: The functionality of the transparent service application for uploading event records from the alcohol interlock to a register or broker may be incorporated into the alcohol interlock. In this case the alcohol interlock uploads the event records to the register or boker.

3.8
opaque service application
service application that is able to decrypt the event records and performs the required conversion of event records

3.9
adjustment
operation that calibrates and/or adjusts the sensor systems, sets parameters and/or changes the firmware of the alcohol interlock

3.10
register
central register of event records, which stores the event records for future use

Note 1 to entry: The register is usually operated by the alcohol interlock manufacturer and/or the authorities.

3.11
broker
processing centre which converts the records into a required format and then sends them to the register or the service application

Note 1 to entry: The broker is usually operated by the service provider of the alcohol interlock.

3.12
security target
description and analysis of the assets, the threats to those assets, the countermeasures (in the form of security objectives) and a demonstration that the countermeasures are sufficient to counter the threats

Note 1 to entry: For details see CCp1, clause 7.1.1.

3.13
security objective
concise statement of the intended solution to the problem defined by the security problem definition

Note 1 to entry: For details see CCp1, clause A.7.

3.14
security problem definition
statement which in a formal manner defines the nature and scope of the security that the alcohol interlock and the service application are intended to address, consisting of a combination of threats to be countered by the alcohol interlock and the service application, the organizational security policies enforced by the alcohol interlock and the service application, and the assumptions that are upheld for the alcohol interlock and the service application and their operational environment

Note 1 to entry: For details see CCp1, clause A.6.

3.15
operational environment
environment in which the alcohol interlock and the service application are operated, containing all entities that the alcohol interlock and the service application interact with, such as broker, register service centre, vehicle, driver

4 General

4.1 Use of the alcohol interlock

Before the engine of the vehicle can start, the driver has to deliver an accepted breath sample into the handset. If the measured alcohol concentration is equal to or above the limit value, the control unit does not allow the vehicle engine to start.

At random intervals while driving, the driver may have to deliver an additional accepted breath sample into the handset. Passing or failing a breath alcohol test generates event records. Additionally, other events may generate event records (e.g. interruption of power to the control unit, or vehicle motion without starting of the motor, indicating bypass of the alcohol interlock).

At set intervals, when the memory of the alcohol interlock fills up, or after certain events the handset instructs the driver to go to a service centre. These service centres (which are for drink-driving-offender programmes normally certified by the government) possess a service application. Service centre personnel can use the service application to read out (download) the encrypted event records from the alcohol interlock.

NOTE The service application may or may not decrypt these event records (see Clause 5).

The service application sends out the event records:

– directly to the register, or

– to the broker which sends the event records to the register, or

– to the broker which sends the event records back to the service application and which then sends it to the register.

The service application requires a confirmation from the register and/or broker that it has received the event records. Upon reception of this confirmation, the service centre personnel may use the service application to delete the event records by erasing the data memory in the alcohol interlock.

4.2 Major security features

The alcohol interlock has the following major security features:

– The alcohol interlock is able to detect events (for example starting the vehicle engine or failed breath test) and store these events;

– Authenticated service personnel can use the service application to read out these event records and send them onwards. The service personnel can also use the service application to delete the event records and erase the data memory;

– All parts of the alcohol interlock protect the event records against unauthorized modification, deletion, insertion and disclosure.

4.3 Hardware, software and firmware not being part of the alcohol interlock and the service application

The alcohol interlock requires installation in a vehicle.

The service application may require an operating system and computer or similar setup in order to function. The security target shall clarify the required hardware, software or firmware (if applicable) required for the service application.

NOTE This depends on the class of the alcohol interlock (see Clause 5).

5 Alcohol interlock classes

5.1 General

This European Standard defines different classes of alcohol interlocks with their service application (A, B1, B2, C1, C2 and D), each of which has slightly different requirements and objectives.

The security target shall define the class of the alcohol interlock (as part of the alcohol interlock overview).

This difference in classes is caused by the following facts.

– The register has a strictly defined format in which it wishes to store event records. As there is no standard for this format yet, each country or organization tends to use its own proprietary format.

– The alcohol interlock may not be able to support all of these formats.

If the alcohol interlock does not support the required format, the files have to be converted somewhere:

– either in the service application, or

– at the broker.

As event records can only be converted when they are not encrypted, they are very vulnerable to unauthorized reading or modification at that point, so special care shall be taken to prevent this.

There may also be alcohol interlocks only using the service application, but not using a register and/or broker, or alcohol interlocks not storing event records at all.

5.2 Class A: transparent service application without broker

Transparent refers to the fact that the service application is not able to decrypt the event records.

This class of alcohol interlocks is characterized by end-to-end encryption between the alcohol interlock and the register. The alcohol interlock already generates the event records in the correct format required by the register. This is depicted in Figure 2.

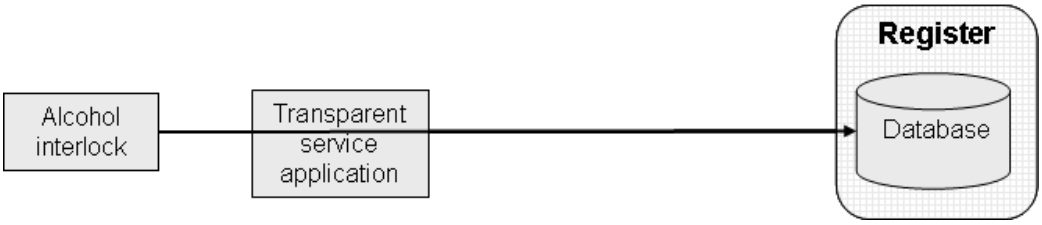

**Figure 2 – Class A alcohol interlock:
the alcohol interlock generates the correct format for the register**

In class A alcohol interlocks:

– the service application never gets access to the unencrypted event records and therefore the service application itself requires relatively little protection;

– there is no broker, so threats for the broker are not relevant and there are no security objectives for the broker.

5.3 Class B: transparent service application with broker

Transparent refers to the fact that the service application is not able to decrypt the event records.

For this class of alcohol interlocks, the broker performs the required conversion. This means that the broker has access to unencrypted event records, and should therefore protect them.

Two subclasses of class B alcohol interlocks are to be distinguished:

– *Class B1 alcohol interlocks:*

The service application sends the event records to the broker. The broker converts the event records, and sends the converted event records onwards to the register. This is depicted in Figure 3.

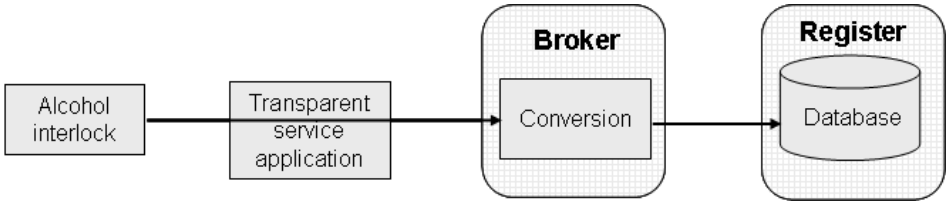

**Figure 3 – Class B1 alcohol interlock:
the broker converts and sends to the register**

– *Class B2 alcohol interlocks:*

The service application sends the event records to the broker. The broker converts the event records, and sends the converted event records back to the service application. The service application then sends the converted event records onwards to the register. This is depicted in Figure 4.