Alcohol Interlock Protection Profile v1.0

August 31, 2010

About this Protection Profile

The Sponsor for this Protection Profile is the Ministry of Transport, Public Works and Water Management of the Netherlands.

For technical enquiries, please contact the Protection Profile authors at:

Brightsight BV
The Netherlands
info@brightsight.com

Document history

Version	Date	Comment
0.5	October 27, 2009	First complete version.
0.6	November 3, 2009	Clarified cryptographic requirements, submitted to JIL.
0.7	December 11, 2009	Made some final adjustments, ready for international submission
0.8	March 15, 2010	Made some adjustments after discussion with V&W. Submitted for evaluation.
0.9	March 22, 2010	Includes final V&W terminology adjustments and comments from first evaluation round
0.99	May 17, 2010	Class B was split into Class B1 and Class B2 to allow more flexible communication between TOE, Broker and Register. This version is currently submitted for certification.
1.0	August 31, 2010	Corrected CB comments, added minor clarifications to TOE description, changed style to reflect the PP ownership.

References

[AV23] G.W. van Blarkom en J.J. Borking, Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen 23, Registratiekamer, 2001 (in Dutch)

[CCp1] Common Criteria for IT Security Evaluation, Part 1, v3.1r3, July 2009

[CCp2] Common Criteria for IT Security Evaluation, Part 2, v3.1r3, July 2009

[CCp3] Common Criteria for IT Security Evaluation, Part 3, v3.1r3, July 2009

[CEMe] Common Methodology for IT Security Evaluation, v3.1r3, July 2009

[EN50] NEN-EN50436-1, Alcohol interlocks: Test methods and performance requirements, Part 1: Instruments for drink-driving-offender programs, 2005

[RAIL] Requirements Alcohol Interlock, Annex 2 van de Ministeriële Regeling Voertuigen, 2009 (in Dutch)

[REPO] Criteria voor Ketenbeveiliging Alcoholslot, Brightsight, 2009 (in Dutch).

Content

1 PP Introduction

1.1 PP Reference

This is the Alcohol Interlock Protection Profile, version 1.0, dated August 31, 2010.

1.2 TOE Overview

An Alcohol Interlock[1] is a device that seeks to ensure that drivers are unable to use their car when they are intoxicated: before they are able to start their car they have to breathe into the Interlock and when this breath contains more than the allowed amount of alcohol, the car will not start.

NB: The quality of the alcohol detection process and whether it can be circumvented using chemicals, sucking on the device instead of breathing etc. are certified as part of another standard (EN-50436-1 [EN50]) and are therefore out of the scope of this Protection Profile.

In this Protection Profile, the Alcohol Interlock (the TOE) consists of three parts:

- A Handset: this is located inside the driver compartment of the car, it contains an alcohol sensor, and is able to interact with the driver
- An Onboard Unit (OBU): this is usually located inside the engine compartment of the car, and is used to store audit records and prevent the starting of the car without a successful alcohol test having been carried out. The OBU is connected to the car: these connections are considered to be part of the OBU.
- A Readout Application: this is located inside a Garage (one Garage can serve thousands of cars fitted with interlocks). The Readout Application is used for functions such as[2] calibration, adjustment and readout of the alcohol interlock, as well as for uploading settings to and recording data and observations in the alcohol interlock, or uploading data from the alcohol interlock to the Register or Broker (see further)

[1] This is the TOE type.

[2] A readout application can have some or all of these functions, depending on its implementation and TOE Class (see section 1.3)

The TOE is depicted in Figure 1:

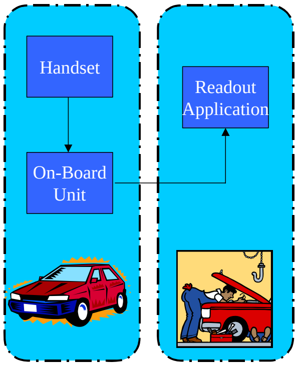


Figure 1: The TOE[3]

The Readout Application sends out the records to one of two places:

1. the Register: this is a central governmental register of records, which stores the records for future use
2. a Broker: this is a processing center (usually run by the developer of the TOE), which converts the records into the correct format and then sends them to the Register (see above). This can be done either:
   a. directly: the Broker sends the records directly to the Register, or
   b. indirectly: the Broker sends the records back to the Readout Application who then sends the records to the Register

Neither the Register, nor the Broker is considered to be part of the TOE. The TOE, Register and Broker are depicted in Figure 2:

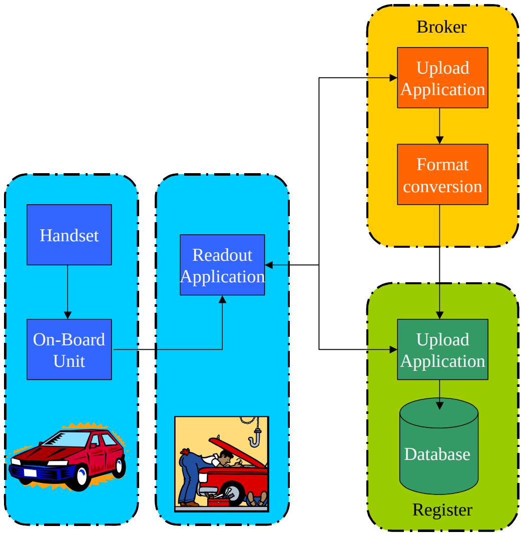


Figure 2: The TOE, the Register and the Broker

[3] In this, and all other figures, the direction of the arrows indicates the flow of records.

1.2.1 Usage

Before a car can start, the driver must breathe into the handset. If the test is negative, the OBU will not allow the car to start. At random intervals, during driving, the driver must again breathe into the handset. Passing or failing a test generates audit records. In addition, some other events generate audit records (e.g. interruption of power to the OBU, or the car is in motion without being started, indicating bypass of the TOE).

At set intervals, or when the memory of the OBU fills up, the Handset instructs the driver to go to the Garage. These Garages (which are certified by the government) possess a Readout Application. Authenticated Garage employees can use the Readout Application to read out (download) the encrypted[4] audit records from the OBU.

These audit records are then sent to either:

- the Broker (which processes them and sends them to the Register, either directly or indirectly through the Readout Application), or
- directly to the Register.

Once the Register receives the audit records it will send a confirmation to the Readout Application (if applicable via the Broker). Upon reception of this confirmation, the authenticated Garage employee uses the Readout Application to delete the audit records, e.g. by erasing the OBU memory.

1.2.2 Major security features

The TOE has the following major security features:

- The Handset and OBU parts of the TOE are able to detect events (starting the car, failed breath test etc.) and store these events[5]
- Authenticated users can use the Readout Application of the TOE to read out these events and send them onwards. These users can also use the Readout Application to delete the events/erase the memory.
- All parts of the TOE protect the events against unauthorized modification, deletion, insertion and disclosure.

1.2.3 Non-TOE Hardware/Software/Firmware

The Handset and the OBU require a car. The Readout Application may require an OS/workstation or similar setup to execute on[6].

Application Note: The ST shall clarify (as part of the TOE overview):

- The specific makes of cars that the TOE claims to be suitable for
- The required non-TOE Hardware/Software/Firmware (if applicable) required for the Readout Application

[4] The Readout Application may or may not decrypt these records. See section 1.3 for details.

[5] Note that the quality of the alcohol test is not subject of this PP, but is arranged through certification against another standard (EN50436-1).

[6] This depends on the Class of the TOE (see section 1.3).

1.3 TOE Classes

This Protection Profile defines five different classes of TOEs (A, B1, B2, C1 and C2), each of which has slightly different requirements and objectives.

Application Note: The ST shall define the Class of the TOE (as part of the TOE Overview).

This difference in Classes is caused by the fact that:

- The Register has a strictly defined format in which it wishes to store data. As there is no standard for this format yet, each country or organization will tend to use its own proprietary format.
- The Handset/OBU may not be able to support all of these formats

If the Handset/OBU does not support the required format, the files have to be converted somewhere:

- either in the Readout Application,
- or at the Broker.

As records can only be converted when they are not encrypted, they are very vulnerable to being read or modified at that point, so special care must be taken to prevent this.

1.3.1 Class A: Transparent Readout Applications without Broker

This class of TOEs is characterized by an end-to-end encryption between the OBU and the Register.

The OBU already contains the records in the correct format required by the Register. This is depicted below:

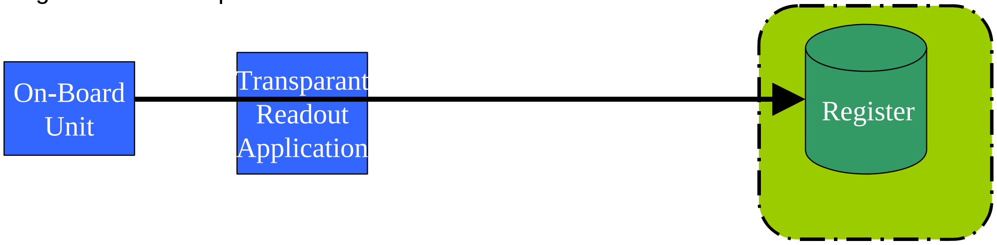


Figure 3: Class A: The OBU contains the correct format

In Class A TOEs:

- the Readout Application never gets access to the records in clear text and therefore the Readout 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

1.3.2 *Class B: Transparent[7] Readout Applications with Broker*

For this class of TOEs, the Broker will perform the required conversion. This means that the Broker will have access to unencrypted records, and must therefore protect them. We distinguish between two subclasses of TOEs:

Class B1 TOEs

The Readout Application will send the records to the Broker. The Broker converts the records, and sends the converted records onwards to the Register. This is depicted below:

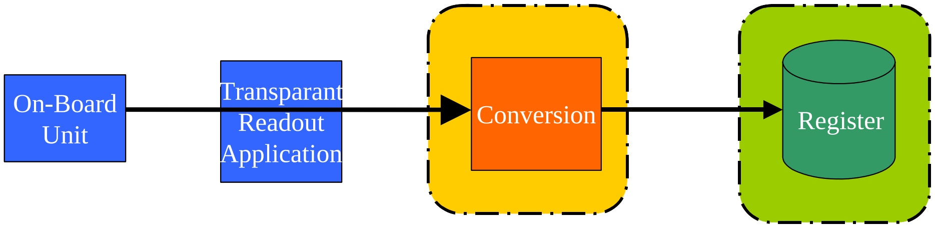


Figure 4: Class B1: The Broker converts and sends to the Register.

Class B2 TOEs

The Readout Application will send the records the Broker. The Broker converts the records, and sends the converted records back to the Readout Application. The Readout Application then sends the converted records onwards to the Register. This is depicted below:

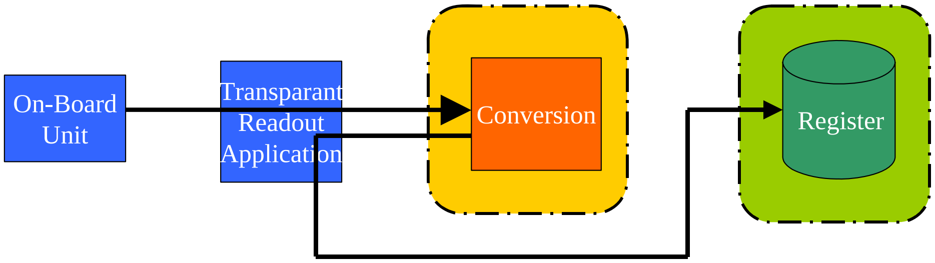


Figure 5: Class B2: The Broker converts and sends to the Readout Application

In Class B TOEs:

- the Readout Application never gets access to the records in clear text and therefore the Readout Application itself requires relatively little protection
- there is a Broker required, so there are threats and objectives for the Broker

1.3.3 *Class C: Opaque Readout Applications*

For this class of TOEs, the Readout Application performs the required conversion. This means that the Readout Application will have access to unencrypted records, and must therefore be able to protect them. We distinguish between two subclasses of TOEs:

[7] "Transparent" refers to the fact that the Readout Application is not able to decrypt the records.

Class C1 TOEs:

The TOE itself must provide the protection. This means that the Readout Application must partly consist of some sort of tamper-evident/tamper-responsive hardware.

Class C2 TOEs

The environment of the TOE must provide the protection. The Readout Application may then be a simple software application running on a non-TOE workstation, but the environment of that workstation must meet stringent requirements to be able to protect the records.

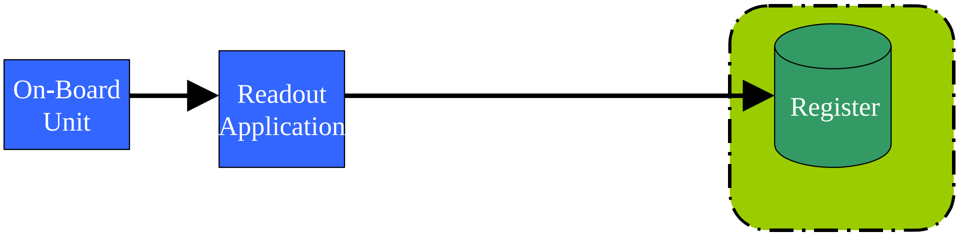


Figure 6: Class C1 and C2: The Readout Application converts.

Neither C1 nor C2 utilizes a Broker: so threats for the Broker are not relevant and there are no security objectives for the Broker.

2 Conformance Claims

This PP conforms to:

- CC, version 3.1R3, as defined by [CCp1], [CCp2], [CCp3] and [CEMe].
- CC Part 2 as CC Part 2 conformant
- CC Part 3 as CC Part 3 conformant

This PP conforms to no other PPs.
This PP conforms to EAL 3+ALC_FLR.2, and to no other packages.
PPs or STs that conform to this PP shall apply strict PP-conformance.

3 Security Problem Definition

This PP only uses threats and does not use organizational security policies or assumptions. To allow other parties to understand the scope and completeness of the PP, a fairly sizable list of threats has been included.

3.1 Assets

The purpose of the alcohol interlock is to protect the following four *assets*:

1. The fact that an intoxicated driver cannot start a car without this being prevented and/or detected
2. The integrity of the audit records: To allow detection as in (1) above: so deletion/modification of audit records should not be possible
3. The non-repudiation of the records, so they constitute proof in legal procedures: therefore unnoticed deletion/modification/insertion of audit records should not be possible
4. The confidentiality of the audit records: to protect the privacy of the driver

3.2 Threat Agents

The assets are threatened by the following threat agents:

1. The driver and/or agents in his employ: the driver may wish to drive while intoxicated, or seek to prevent detection that he has done so or attempted to do so
2. Parties that seek to bring the system into disrepute: if parties can prove they modified or inserted audit records without this being detected, this will invalidate the non-repudiation status of all other records. If they can show that they can delete records without this being detected they will undermine the reputation of the system.
3. Parties that seek to invade the privacy of persons. E.g. a journalist might be interested in finding out that a well-known political figure attempted to drive while intoxicated.

For each of the threats below, it should be obvious to which asset and threat agent they apply. To maintain readability, this has not been listed with every threat.

3.3 Threats

This PP provides a detailed analysis of threats: both directly to the TOE and to the environment of the TOE.

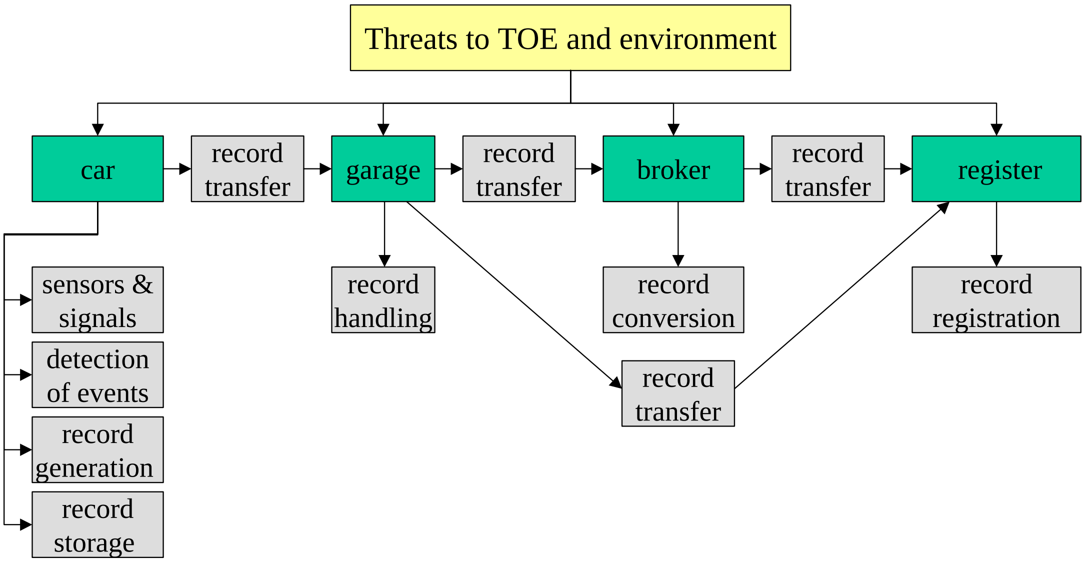


Figure 7: Threats to the TOE and the Environment.

The threats are grouped into classes: each gray box in the picture above depicts a class of threats. Each class of threats is described in a separate subsection above.

3.3.1 Messing with the sensors and the signals to the car (I)

This class of threats attempts to fool the alcohol sensor and/or the connections between the OBU and the car. We distinguish:

- ▢ I.1: Let other people breathe through the handset
- ▢ I.2: Chemical/physical attacks that change/modify/substitute the air breathed into the handset[8]
- ▢ I.3: The handset and OBU are somehow bypassed, allowing the car to be started, regardless of whether there was a (successful) alcohol test.

3.3.2 Prevention of detection of events (II)

This class of threats attempts to prevent the detection of the relevant events. We distinguish:

- ▢ II.1 Failure to detect any relevant event.

Application Note: For the Netherlands, the relevant events are listed in [RAIL]

[8] This PP only looks at the basic attacks (those listed in the EN 50436-1 standard [EN50]). More advanced threats to the alcohol sensor are outside the scope of this Protection Profile.

3.3.3 Prevention of generation of audit records[9] (III)

This class of threats attempts to prevent audit records from being generated or being correctly generated, even though an auditable event has occurred.
We distinguish:

- III.1 Failure to generate an audit record, e.g. by:
  - Disconnecting the handset from the On-Board Unit or otherwise interfering with the connection between them
- III.2 Modification of generation of an audit record, e.g. by:
  - Applying extreme external conditions, such as voltage spikes, high/low temperature, or
  - Physical modification of the alcohol interlock, or
  - Modifying information between handset and OBU as it is transferred between them
- III.3 Failure to generate an audit record due to storage overflow
- III.4 Failure to generate an audit record because the sensors have been deliberately miscalibrated

3.3.4 Failure to correctly store audit records in the OBU (IV)

This class of threats attempts to modify/delete/create/read audit records while they are being stored by the interlock. We distinguish:

- IV.1 Undetected modification of audit records while being stored. This includes:
  - Accidental modification (e.g. memory errors)
  - Deliberate modification
- IV.2 Undetected deletion of audit records while being stored. This includes:
  - Deletion of (part of) the memory contents
  - Removal/replacement/damaging/destruction of the memory itself
- IV.3 Undetected insertion of audit records while being stored
- IV.4 Unauthorized reading of audit records while being stored. This includes:
  - Reading the data directly from the integrated circuits where it resides
  - Authorized deletion, but the records have not yet been received by the Register

3.3.5 Failure to correctly transfer audit records between Onboard Unit and Readout Application (V)

This class of threats attempts to modify/delete/create/read audit records while they are being transferred between the Onboard Unit and the Readout Application. We distinguish:

- V.1: Modification of audit records in transit between On-board unit and Readout Application. This includes:

[9] This Protection Profile uses the Common Criteria term “audit records” instead of the term “event records”, which is more common in the Alcohol Interlock field.

    - Accidental modification (e.g. transmission errors)
    - Reading the data with a wrong version of the Read Out Application, thus misinterpreting the data
    - Sending an invalid or truncated set of audit records
    - Deliberate modification
- V.2: Deletion of audit records in transit between On-board unit and Readout Application
- V.3: Insertion of audit records in transit between On-board unit and Readout Application
- V.4: Reading of audit records in transit between On-board unit and Readout Application. This includes:
    - Reading the audit records by other means than a Readout Application
    - Reading the audit records by a Readout Application, but by a person that is not authorized to use this Readout Application
- V.5: Deletion of audit records through application of the Readout Application before these audit records have been correctly received by the Register.[10]

3.3.6 Failure to correctly handle the records in the Readout Application (VI)

This class of threats attempts to modify/delete/create/read audit records while they are in the Readout Application. We distinguish:

- VI.1 Modification of audit records while in the Readout Application. This includes:
    - Accidental modification (e.g. storage or, conversion or processing errors)
    - Deliberate modification
- VI.2 Deletion of audit records while in the Readout Application
- VI.3 Insertion of audit records while in the Readout Application
- VI.4 Reading of audit records while in the Readout Application. This includes:
    - The Readout Application retaining copies of parts of audit records which may be read at a later date. This could be explicit copies of records, but also accidental copies left in swap files, deleted disk sectors etc.

3.3.7 Failure to correctly transfer audit records between Readout Application and Register (VII)

Application Note: These threats are not relevant for Class B1 TOEs, as these TOEs never transfer records between Readout Application and Register, but always use a Broker as an intermediary.

[10] This includes solutions that make a backup in the OBU whenever the OBU is read out, overwriting the old backup. By reading out the OBU twice, first the data is moved to the backup, and then it is overwritten, thus deleting it.

This class of threats attempts to modify/delete/create/read audit records while they are being transferred between the Readout Application and the Register. We distinguish:

- VII.1: Modification of audit records in transit between Readout Application to Register. This includes:
  - Accidental modification (e.g. transmission errors)
  - Sending an invalid or truncated set of audit records
  - Deliberate modification
- VII.2: Deletion of audit records in transit between Readout Application to Register
- VII.3: Insertion of audit records in transit between Readout Application to Register. This includes:
  - Audit records being sent twice (either deliberately or by accident)
  - Unauthenticated or unknown parties sending audit records
- VII.4: Reading of audit records in transit between Readout Application to Register

3.3.8 Failure to correctly register records at the Register (VIII)

This class of threats attempts to modify/delete/create/read audit records while they are at the Register. We distinguish:

- VIII.1 Modification of audit records while at the Register. This includes:
  - Accidental modification (e.g. storage, processing or conversion errors)
  - Deliberate modification
- VIII.2 Deletion of audit records while at the Register
- VIII.3 Insertion of audit records while at the Register
- VIII.4 Reading of audit records while at the Register

3.3.9 Failure to correctly transfer audit records between Readout Application and Broker (IX)

Application Note: These threats are only relevant for Class B TOEs, as the other classes do not use a Broker. Note that in the case of B2 TOEs, these threats also apply to the records the Broker sends back to the Readout Application..

This class of threats attempts to modify/delete/create/read audit records while they are being transferred between the Readout Application and the Broker.

We distinguish:

- IX.1: Modification of audit records in transit between Readout Application and Broker. This includes:
  - Accidental modification (e.g. transmission errors)
  - Sending an invalid or truncated set of audit records
  - Deliberate modification
- IX.2: Deletion of audit records in transit between Readout Application and Broker

- IX.3: Insertion of audit records in transit between Readout Application and Broker. This includes:
  - Audit records being sent twice (either deliberately or by accident)
  - Unauthenticated or unknown parties sending audit records
- IX.4: Reading of audit records in transit between Readout Application and Broker. This includes:
  - Audit records being sent by the Readout Application to the wrong Broker
  - Audit records being sent by the Broker to the wrong Readout Application

3.3.10 Failure to correctly convert records at the Broker (X)

Application Note: These threats are only relevant for Class B TOEs, as the other classes do not use a Broker.

This class of threats attempts to modify/delete/create/read audit records while they are being converted by the Broker. We distinguish:

- X.1 Modification of audit records while at the Broker. This includes:
  - Accidental modification (e.g. storage, processing or conversion errors)
  - Deliberate modification
- X.2 Deletion of audit records while at the Broker
- X.3 Insertion of audit records while at the Broker
- X.4 Reading of audit records while at the Broker

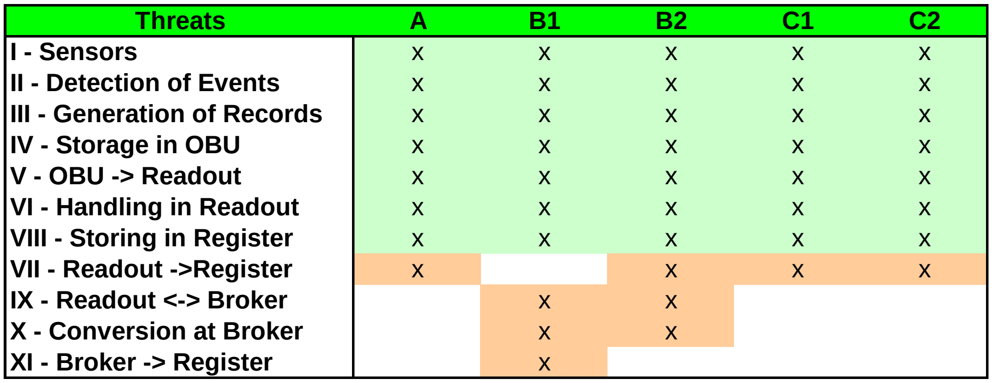
3.3.11 Failure to correctly transfer audit records between Broker and Register (XI)

Application Note: These threats are only relevant for Class B1 TOEs, as this is the only class that uses a Broker that transfers records to the Register.

This class of threats attempts to modify/delete/create/read audit records while they are being transferred between the Broker and the Register. We distinguish:

- XI.1: Modification of audit records in transit between Broker and Register. This includes:
  - Accidental modification (e.g. transmission errors)
  - Deliberate modification
- XI.2: Deletion of audit records in transit between Broker and Register.
- XI.3: Insertion of audit records in transit between Broker and Register. This includes:
  - Audit records being sent twice (either deliberately or by accident)
  - Unauthenticated or unknown parties sending audit records
- XI.4: Reading of audit records in transit between Broker and Register

The following table provides an overview of the threats versus the TOE Classes defined in section 1.3. It shows the common threats in green, and the threats that are not relevant for one or more Classes in light brown.



Threats	A	B1	B2	C1	C2
I - Sensors	x	x	x	x	x
II - Detection of Events	x	x	x	x	x
III - Generation of Records	x	x	x	x	x
IV - Storage in OBU	x	x	x	x	x
V - OBU -> Readout	x	x	x	x	x
VI - Handling in Readout	x	x	x	x	x
VIII - Storing in Register	x	x	x	x	x
VII - Readout ->Register	x		x	x	x
IX - Readout <-> Broker		x	x		
X - Conversion at Broker		x	x		
XI - Broker -> Register		x			

4 Security Objectives

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in section 6.1 of this Protection Profile.

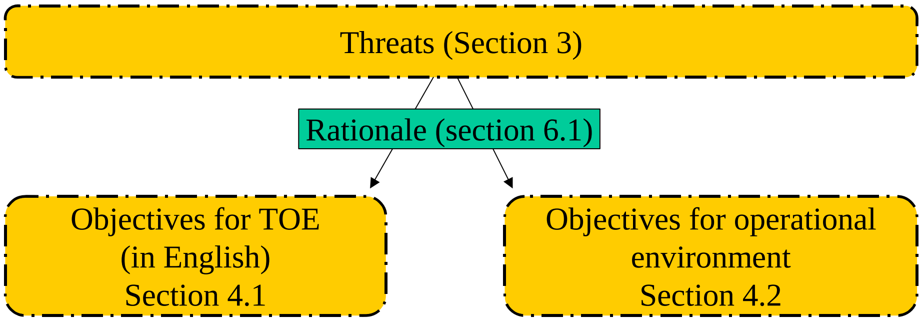


Figure 8: Relations between threats and security objectives

4.1 Security objectives for the TOE

O.DETECT_EVENTS

The combination of Handset and OBU shall detect all events required by the applicable laws and regulations.

Application Note: For the Netherlands, the required events are listed in [RAIL].

O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_OBU

The Handset and OBU shall protect information about detected events as this is exchanged between them against insertion, deletion and modification.

O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU

The OBU shall store all required information for each event in audit records in the OBU. Each audit record shall contain at least:

- The information required by the applicable laws and regulations.
- A unique consecutive number for each audit record.

The OBU shall store all audit records in such a way that they cannot be read or modified by unauthorized entities.

The OBU shall encrypt[11] all audit records before allowing them to be read out[12] in such a way that they cannot be read or modified by unauthorized entities.

Application Note: For the Netherlands, the required events are listed in [RAIL].

O.TAMPER_EVIDENT_HANDSET_AND_OBU

The Handset and OBU shall be tamper-evident. Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

Application Note: Note that the connections from the OBU to the car are considered part of the OBU and therefore must also be tamper evident.

O.TAMPER_EVIDENT_READOUT_APPLICATION (Only for Class C1 TOEs)

The Readout Application shall be tamper-evident. Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

O.NO_OVERFLOW_IN_OBU

When the memory of the OBU is filled with audit records for:

- 90%, the OBU shall issue an early recall warning to the driver
- 100%, the OBU shall no longer allow the car to start

O.OBU_AND_READOUT_APPLICATION

The OBU shall allow only the Readout Application to:

- Read out audit records from the OBU
- Delete audit records from the OBU
- Calibrate the OBU and the Handset

O.READOUT_APPLICATION_AUTHENTICATION

Before a human user can use the Readout Application, this user must first be identified and authenticated.

Application Note: O.READOUT_APPLICATION_AUTHENTICATION does not specify that the TOE must perform I&A itself. It is specifically allowed for the environment (the Operation System, a remote webserver or other entity) to perform this I&A.

[11] Note that this encryption must also protect against modification. The consecutive numbers may solve part of this, but other measures (MAC, CRC inside the encryption, CBC-mode etc.) may also be necessary, depending on the implementation.

[12] Note that it is allowed to encrypt the audit records before storing them, but it is also allowed to store the audit records unencrypted and encrypt them as they are being read out. In both cases they must be stored in such a way that they cannot be read or modified by unauthorized entities, but this is likely to be easier to implement when they are encrypted before being stored.

O.READOUT_APPLICATION_PROTECT_RECORDS

The Readout Application shall not allow its users (or other entities) to insert, modify or read audit records from the Readout Application. This includes reading of audit records after they have been sent onwards.

O.SEND_TO_CORRECT_PARTY

The Readout Application shall send the audit records only to the correct party in the correct manner.

The Readout Application shall be able to receive a confirmation that the audit records have been correctly received.

- For Class B1 TOEs, the audit records shall be sent to the Broker, using the method specified by the Broker, and the confirmation will be received from the Broker.
- For Class B2 TOEs, the audit records shall be sent to the Broker, using the method specified by the Broker, then the records received by the Broker shall be sent to the Register, using the method specified by the Register, and the conformation shall be received from the Register.
- For all other Classes of TOEs, the audit records shall be sent to the Register, using the method specified by the Register, and the confirmation will be received from the Register.

4.2 Security Objectives for the Operational Environment

4.2.1 General Security Objectives for the Operational Environment

OE.INTERLOCK_50436-1

The interlock shall be certified against EN-50436-1 [EN50].

Application Note: For the Netherlands, the amendments to EN50436-1 that are listed in [RAIL] shall apply.

OE.DELETE_ONLY_AFTER_CONFIRMATION

The human user of the Readout Application will only delete audit records from the OBU when a confirmation has been received that these audit records have been correctly received.

OE.PROTECTED_READOUT_APPLICATION (Only for Class C2 TOEs)

The Garage environment shall use a combination of technical and organizational means to ensure that unauthorized modification, deletion, insertion and/or reading of records that are processed by the Garage is impossible.

Application Note: For the Netherlands, this must mean that every Garage that uses the Readout Application must meet all applicable requirements of [AV23], risk class 2.

4.2.2 Security objectives for the Register (in the Operational Environment)

Application Note: For the Netherlands, the mandatory methods for meeting the security objectives for the Register are described in [REPO].

OE.REGISTER_PROTECT_INCOMING_RECORDS

The Register shall provide an application to entities that wish to provide audit records to it. This application shall provide:

- Authentication of the sender
- Detection of any modification or insertion of audit records while in transit
- Prevent third parties reading the audit records while in transit

The Register shall accept only audit records provided to it through this application.

OE.REGISTER_PROTECT_RECORDS

The Register shall use a combination of technical and organizational means to prevent unauthorized modification, deletion, insertion and/or reading of audit records that are stored in the register.

Application Note: For the Netherlands, the required information and format are listed in [RAIL].

OE.REGISTER_CHECK_AND_CONFIRM

The Register shall check all audit records that it receives (after possibly converting them) for completeness and reply the result of this check to the sender of the records (either Broker or Readout Application).

4.2.3 Security objectives for the Broker (in the Operational Environment)

Application Note: All of the security objectives in this section are only relevant for Class B TOEs. All other classes do not have to meet these security objectives, since they do not use Brokers.

Application Note: For the Netherlands, the mandatory methods for meeting the security objectives for the Broker are described in [REPO].

OE.BROKER_PROTECT_INCOMING_RECORDS

The Broker shall offer a means of transfer of data from Readout Applications to itself (e.g. a https connection). This means of transfer shall ensure that:

- Authentication of the sender
- The events cannot be read by unauthorized entities while in transfer
- Modification, insertion and deletion of events can be detected

OE. BROKER_PROTECT_RECORDS

The Broker shall use a combination of technical and organizational means to prevent unauthorized modification, deletion, insertion and/or reading of records that are processed by the Broker.

The Broker shall securely delete all copies of (parts of) old and new audit records once the Register indicates that the new audit records have been received correctly.

OE.BROKER_CORRECT_CONVERSION

The Broker shall process the audit records into new audit records. The Broker shall demonstrate by rigorous testing that:

- The new audit records contain all the information required by the applicable laws and regulations.
- The new audit records are in the required format.
- The information in the new audit records is correctly derived from the information in the old audit records.

Application Note: For the Netherlands the required format is listed in [RAIL].

OE. BROKER_SEND_TO_CORRECT_PARTY

The Broker shall send the new audit records only to the correct party:

- For Class B1 TOEs to the Register, using the Register supplied application)
- For class B2 TOEs, to the Readout Application. Before sending the new audit records, the Broker shall encrypt the records such that:
  - The events can only be read by the Register
  - Modification, insertion and deletion of the events can be detected

OE.BROKER_RELAY_CONFIRMATION

The Broker shall relay the result of the check by the Register to the Readout Application.

5 Security Requirements

5.1 Definitions

The following terms are used in the security requirements:

Subjects/External Entities:

- Handset
- OBU
- Readout Application
- Register
- Broker

All of these are defined in the TOE Overview. They have no security attributes

Objects:

- Audit records
- OBU (treated as object by the calibrate operation)
- Handset (treated as object by the calibrate operation)

All of these are defined in the TOE Overview. They have no security attributes.

Operations

- Broker-send: An operation that sends data to the Broker by a method approved by that Broker
- Calibrate: An operation that calibrates the sensors in OBU and Handset
- Convert: An operation that creates a new set of audit records from an old set in a different syntactic format
- Delete: An operation that permanently removes audit records
- Read: An operation that reads non-encrypted audit records
- Readout: An operation that makes a local copy of encrypted audit records without decrypting them.
- Register-send: An operation that sends data to the Register by a method approved by that Register
- Receive: An operation that receives a confirmation or a set of audit records

5.2 Security Functional Requirements

These security requirements are a more exact description of the Security Objectives for the TOE listed in section 4.1). They are written in a special “security language” defined in the Common Criteria. The use of this language ensures that the requirements do not allow for ambiguity or misinterpretation by an evaluator and that they are testable.

The evaluation of an Alcohol Interlock will determine whether or not a specific Alcohol Interlock meets the security functional requirements in this section.

A demonstration that the combination of all of these security functional requirements indeed addresses the security objectives for the TOE may be found in section 6.2 of this Protection Profile.

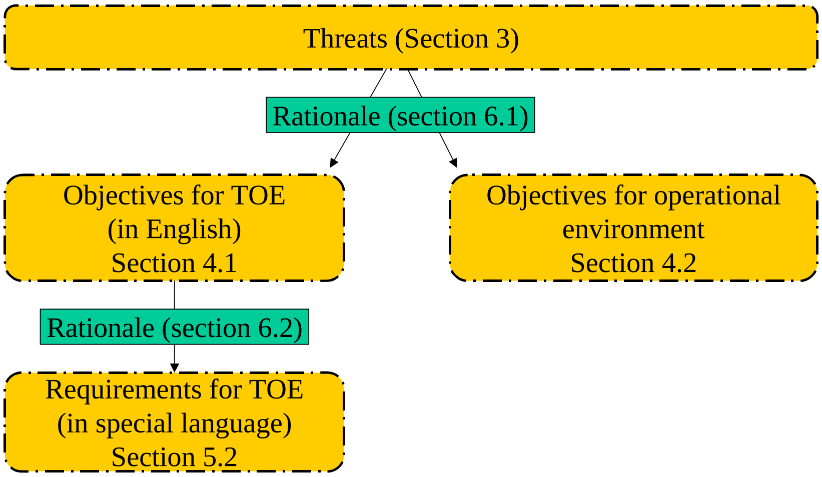


Figure 9: Relations between threats, security objectives and security functional requirements

Application Note: Throughout this section, the term TSF has been refined many times to show to which part of the TSF the SFRs apply. These refinements are bolded.

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) -[13]

c) [**deletion of audit records,**
calibration of the OBU and/or Handset,
assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event, **a unique consecutive number**[14]; and

b) for each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Application Note: The assignment in 1c shall be completed to comply with the applicable laws and regulations, but shall include at least the two specifically listed events. 2a may be further refined for the same reason.

Application Note: For the Netherlands, the events and information are listed in [RAIL].

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The **OBU** shall protect the stored audit records in the audit trail from unauthorised deletion **and reading**[15].

FAU_STG.1.2 The **OBU** shall be able to [selection: choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The **Handset and OBU** shall **issue an early recall warning to the driver** if the audit trail exceeds **90% of storage space.**

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The **Handset and OBU** shall **ignore audited events** and **prevent the car from starting** if the audit trail is full.

[13] “not specified”was chosen, and the entire element was then refined away for readability.
[14] This is a refinement.
[15] This is a refinement

FCS_COP.1(1) Cryptographic operation

FCS_COP.1.1 The **OBU** shall perform **encryption of audit records before they are read out**[16] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note: See section 5.3 for information on completing this requirement.

FCS_COP.1(2) Cryptographic operation[17]

FCS_COP.1.1 The **Readout Application** shall perform **decryption of audit records** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note: See section 5.3 for information on completing this requirement.

FCS_COP.1(3) Cryptographic operation[18]

FCS_COP.1.1 The **Readout Application** shall perform **encryption of converted audit records** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note: See section 5.3 for information on completing this requirement.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Interlock Policy** on

- **Readout Application, OBU, Handset, Register, Broker**
- **Audit Records**
- **calibrate, convert, delete, read, readout,**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Interlock Policy** to objects based on the following: **Readout Application, OBU, Handset, Register, Broker, Audit Records**[19]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

For all Classes of TOEs:

- **Readout Application may readout audit records from OBU**
- **Readout Application may delete audit records from OBU**
- **Readout Application may calibrate OBU and Handset**

[16] "before they are read out" is a refinement, showing the timing of the encryption
[17] This SFR is only required for Class C1 and C2 TOEs.
[18] This SFR is only required for Class C1 and C2 TOEs.
[19] None of these has security attributes.

For Class A TOEs:

- **Readout Application may register-send audit records to Register**
- **Register may read audit records**
- **Readout Application may receive confirmation from Register**

For Class B1 TOEs:

- **Readout Application may broker-send audit records to Broker**
- **Broker may read audit records**
- **Readout Application may receive confirmation from Broker**

For Class B2 TOEs:

- **Readout Application may broker-send audit records to Broker**
- **Broker may read audit records**
- **Readout Application may receive and then register-send audit records to Register**
- **Register may read audit records**
- **Readout Application may receive confirmation from Register**

For Class C TOEs:

- **Readout Application may read audit records**
- **Readout Application may convert audit records**
- **Readout Application may register-send audit records to Register**
- **Register may read audit records**
- **Readout Application may receive confirmation from Register**

FDP_ACF.1.3 -[20]
FDP_ACF.1.4 -

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the **Interlock Policy** to prevent the **disclosure and/or undetected**[21] **modification** of **audit records**[22] when **they are**[23] transmitted between **OBU and Readout Application**[24]

FDP_ITT.3 Integrity monitoring

FDP_ITT.3.1 The **Handset and OBU** shall[25] monitor **information about detected events**[26] transmitted between **Handset and OBU**[27] for the following errors: **insertion, modification and deletion**.

FDP_ITT.3.2 Upon detection of an integrity error, the TOE shall [assignment: specify the action to be taken upon integrity error].

Application Note: Modifying or exchanging the handset without being detected and using this to insert, delete or modify information about detected events being sent to the OBU would be a violation of the FDP_ITT.3 requirement.

[20] Assignments in 1.3 and 1.4 were completed with "none" and then refined away for readability.
[21] Refinement to show that modification can only be detected and not prevented.
[22] User data was refined to "audit records" to show which user data is meant
[23] editorial refinement to make the sentence correct English.
[24] "physically separated parts of the TOE" was refined into "Handset and OBU" to show which parts are meant.
[25] As there is no relevant access control policy covering this, part of the SFR was refined away.
[26] User data was refined to "information about detected events" to show which user data is meant
[27] "physically separated parts of the TOE" was refined into "Handset and OBU" to show which parts are meant.

FDP_RIP.1 Subset residual information protection[28]

FDP_RIP.1.1 The **Readout Application** shall ensure that any previous information content of a resource **in the Readout Application**[29] is made unavailable upon the **deallocation of the resource from** the following objects: **audit records**.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The **Readout Application** shall require each user to be successfully authenticated before allowing any other **Readout Application** -mediated actions on behalf of that user.

Application Note: If the authentication is done in the operational environment, FIA_UAU.2is not required. *FIA_UID.2 User identification before any action*

FIA_UID.2.1 The **Readout Application** shall require each user to be successfully identified before allowing any other **Readout Application** -mediated actions on behalf of that user.

Application Note: If the identification is done in the operational environment, FIA_UID.2 is not required.

FPT_PHP.1(1) Passive detection of physical attack[30]

FPT_PHP.1.1 The **Handset and OBU** shall provide unambiguous detection of physical tampering that might compromise the **Handset and OBU**.

FPT_PHP.1.2 The **Handset and OBU** shall provide the capability to determine whether physical tampering with the **Handset and OBU** has occurred.

Application Note: Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

Application Note: A TOE may detect tampering with the wires leading from the OBU to the car[31] and log this. This is considered to be tamper-evidence as far as this requirement is concerned. Note that just logging is not allowed for tampering with the OBU itself.

FPT_PHP.1(2) Passive detection of physical attack[32] [33]

FPT_PHP.1.1 The **Readout Application** shall provide unambiguous detection of physical tampering that might compromise the **Readout Application**.

FPT_PHP.1.2 The **Readout Application** shall provide the capability to determine whether physical tampering with the **Readout Application** has occurred.

Application Note: Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

[28] This SFR is only required for Class C1 and C2 TOEs.

[29] A refinement to limit this to only the Readout Application

[30] TSF and TSF's devices and elements were refined several times to show which part of the TSF is meant.

[31] These wires are considered to be part of the OBU (see Section 1.2).

[32] This SFR is only required for Class C1 TOEs.

[33] TSF and TSF's devices and elements were refined several times to show which part of the TSF is meant.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The **OBU** shall be able to provide reliable time stamps.

5.3 Cryptographic Algorithms

The TOE performs various cryptographic operations. All of these shall use strong cryptographic algorithms. In this PP, single DES is not considered to be strong, while 3DES, AES, RSA 1024 and greater are considered to be strong. For other algorithms, the developer shall contact the Certification Body.

This PP does not contain the various dependencies of FCS_COP.1, because it does not wish to mandate key management solutions. The ST writer shall still address these dependencies to specify the key management solution.

5.4 Security Assurance Requirements

The Security Assurance Requirements for this Protection Profile are EAL3+ALC_FLR.2.

The reasons for this choice are that:

- EAL 3 is deemed to provide a good balance between assurance and costs: it contains a site audit to examine the developers process and enough information to determine the main security features: cryptographic architecture and tamper-evidence.
- ALC_FLR.2 provides a good structure for the remediation of security flaws: this supports accreditation structures where not every version of a product will be certified.

6 Rationales

6.1 Security Objectives Rationale

The table below lists all threats on the left side. For each threat the objectives are listed that counter this threat, with a short rationale on why they counter this threat.

As this PP does not use OSPs or assumptions, there is no further security objectives rationale.

Messing with the sensors and the signals to the car (I)	
I.1: Let other people breathe through the handset	OE.INTERLOCK_50436-1 ensures that the driver is tested periodically when driving (section 4.7 of EN50436-1 [EN50]). It is still possible for the driver to take a sober passenger, and let him breathe for these tests, but this risk is seen as very unlikely and hence accepted: why would sober people risk their lives as passenger of a drunk driver?
I.2: Basic chemical/physical attacks that change/modify/substitute the air breathed into the handset (the attacks are listed in the 50436-1 standard [EN50])	OE.INTERLOCK_50436-1 explicitly includes this threat in its certification (section 7 of EN50436-1 [EN50]), thereby countering it.
I.3: The handset and OBU are somehow bypassed, allowing the car to be started, regardless of whether there was a (successful) alcohol test.	OE.INTERLOCK_50436-1 specifies that there is either a motion sensor in the OBU (section 4.6 of EN50436-1 EN50]) or detection of start/stop by the OBU. O.DETECT_EVENTS ensures that in both cases this event is detected O. TAMPER_EVIDENT_HANDSET_AND_OBU ensures that neither the OBU nor the connections can be modified to change this without this being evident.
Prevention of detection of events (II)	
II.1 Failure to detect any relevant event	O.DETECT_EVENTS ensures that all relevant events are detected and defines all relevant events for the Dutch situation. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.
Prevention of generation of audit records (III)	
III.1 Failure to generate an audit record e.g. by: Disconnecting the handset from the On-Board Unit or otherwise interfering with the connection between them	O.DETECT_EVENTS ensures that disconnecting the handset will generate an event and will thus be detected. O.PROTECT_EVENTS_BETWEEN_HANDSET_AND _OBU ensures that information between handset and OBU cannot be deleted/modified without this being detected. O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU ensures that an audit record is stored with the correct information O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.

III.2 Modification of generation of an audit record, e.g. by: □ Applying extreme external conditions, such as voltage spikes, high/low temperature, or □ Physical modification of the alcohol interlock, or □ Modifying information between handset and OBU as it is transferred between them	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU ensures that an audit record is stored with the correct information O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_OBU ensures that information between handset and OBU cannot be modified O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this. OE. INTERLOCK_50436-1 proscribes additional environmental tests that support this.
III.3 Failure to generate an audit record due to storage overflow	O.NO_OVERFLOW_IN_OBU specifies the actions needed in case of overflow and impending overflow, thus countering this threat. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the OBU cannot be modified to change this.
III.4 Failure to generate an audit record because the sensors have been deliberately miscalibrated	O.OBU_AND_READOUT_APPLICATION counters this threat by preventing anyone except the Readout Application to perform calibration O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.
Failure to correctly store audit records in the OBU (IV)	
IV.1 Undetected modification of audit records while being stored. This includes: □ Accidental modification (e.g. memory errors) □ Deliberate modification	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU ensures that the audit records cannot be changed by unauthorized entities If encryption is used, it explicitly addresses the fact that the encryption should be done in such a way that modification can always be detected. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.
IV.2 Undetected deletion of audit records while being stored. This includes: □ Deletion of (part of) the memory contents □ Removal/replacement/damaging/destruction of the memory itself	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that a unique consecutive number is stored within the audit record. Therefore one can detect deletion of records, as some of the numbers would go missing. O.OBU_AND_READOUT_APPLICATION assists in this by only allowing the Readout Application to perform a deletion of audit records. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.
IV.3 Undetected insertion of audit records while being stored	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that unauthorized entities cannot modify records and that a unique consecutive number is stored within the audit record. Therefore one cannot create new records from scratch and one cannot replay records. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.

IV.4 Unauthorized reading of audit records while being stored. This includes: □ Reading the data directly from the integrated circuits where it resides □ Authorised deletion,but the records have not yet been received by the Register	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that the records cannot be read by unauthorized entities. O.OBU_AND_READOUT_APPLICATION assists in this by only allowing the Readout Application to readout the audit records from the OBU. O.TAMPER_EVIDENT_HANDSET_AND_OBU ensures that the Handset and OBU cannot be modified to change this.
Failure to correctly transfer audit records between Onboard Unit and Readout Application (V)	
V.1: Modification of audit records in transit between On-board unit and Readout Application. This includes: □ Accidental modification (e.g. transmission errors) □ Reading the data with a wrong version of the Readout Application, thus misinterpreting the data □ Sending an invalid or truncated set of audit records □ Deliberate modification	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies encryption of the events to ensure that they cannot be changed or misinterpreted without this being detectable. O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU also specifies that a unique consecutive number is encrypted within the audit record. Therefore one can detect an invalid or truncated set of records. OE.DELETE_ONLY_AFTER_CONFIRMATION specifies that eventually the records will be deleted from the OBU, further supporting this objective.
V.2: Deletion of audit records in transit between On-board unit and Readout Application	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that a unique consecutive number is encrypted within the audit record. Therefore one can detect deletion of records, as some of the numbers would go missing.
V.3: Insertion of audit records in transit between On-board unit and Readout Application	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that a unique consecutive number is encrypted within the audit record. Therefore one cannot create new records from scratch and one cannot replay records.
V.4: Reading of audit records in transit between On-board unit and Readout Application. This includes: □ Reading the audit records by another means than a Readout Application □ Reading the audit records by a Readout Application, but by a person that is not authorized to use this Readout Application	O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU specifies that the records are encrypted thus making it impossible to read them.

V.5: Deletion of audit records through application of the Readout Application before these audit records have been correctly received by the Register.[34]	OE.REGISTER_CHECK_AND_CONFIRM ensures that the Register will check the records and send back the result. OE.BROKER_RELAY_CONFIRMATION specifies that (if the Broker is used) it will relay the result to the Readout Application. OE.DELETE_ONLY_AFTER_CONFIRMATION specifies that the human user will take care of this. It is not necessarily automatically enforced by the Readout application (although the Readout Application may choose to do so in addition). O.READOUT_APPLICATION_AUTHENTICATION specifies that only authenticated human users can use the Readout Application, lessening the chance that this threat will happen even further.
Failure to correctly handle the records in the Readout Application (VI)	
VI.1 Modification of audit records while in the Readout Application. This includes: □ Accidental modification (e.g. storage or, conversion or processing errors) □ Deliberate modification	O.READOUT_APPLICATION_PROTECT_EVENTS specifies that the Readout Application should protect against modification. O.READOUT_APPLICATION_AUTHENTICATION specifies that only authenticated human users can use the Readout Application, lessening the chance that this threat will happen even further. For Class C1 TOEs, this is supported by O.TAMPER_EVIDENT_READOUT_APPLICATION to protect the records in the Readout Application against physical tampering. For Class C2 TOEs, this is supported by OE.PROTECTED_READOUT_APPLICATION, where the Garage environment protects the records in the Readout Application against tampering.

[34] This includes solutions that make a backup in the OBU whenever the OBU is read out, overwriting the old backup. By reading out the OBU twice, first the data is moved to the backup, and then it is overwritten, thus deleting it.

VI.2 Deletion of audit records while in the Readout Application	O.READOUT_APPLICATION_PROTECT_RECORDS specifies that the Readout Application should protect against deletion. O.READOUT_APPLICATION_AUTHENTICATION specifies that only authenticated human users can use the Readout Application, lessening the chance that this threat will happen even further. For Class C1 TOEs, this is supported by O.TAMPER_EVIDENT_READOUT_APPLICATION to protect the records in the Readout Application against physical tampering For Class C2 TOEs, this is supported by OE.PROTECTED_READOUT_APPLICATION, where the Garage environment protects the records in the Readout Application against tampering.
VI.3 Insertion of audit records while in the Readout Application	O.READOUT_APPLICATION_PROTECT_RECORDS specifies that the Readout Application should protect against insertion. O.READOUT_APPLICATION_AUTHENTICATION specifies that only authenticated human users can use the Readout Application, lessening the chance that this threat will happen even further. For Class C1 TOEs, this is supported by O.TAMPER_EVIDENT_READOUT_APPLICATION to protect the records in the Readout Application against physical tampering For Class C2 TOEs, this is supported by OE.PROTECTED_READOUT_APPLICATION, where the Garage environment protects the records in the Readout Application against tampering.
VI.4 Reading of audit records while in the Readout Application. This includes: □ The Readout Application retaining copies of parts of audit records which may be read at a later date. This could be explicit copies of records, but also accidental copies left in swap files, deleted disk sectors etc.	O.READOUT_APPLICATION_PROTECT_RECORDS specifies that the Readout Application should protect against reading. O.READOUT_APPLICATION_AUTHENTICATION specifies that only authenticated human users can use the Readout Application, lessening the chance that this threat will happen even further. For Class C1 TOEs, this is supported by O.TAMPER_EVIDENT_READOUT_APPLICATION to protect the records in the Readout Application against physical tampering For Class C2 TOEs, this is supported by OE.PROTECTED_READOUT_APPLICATION, where the Garage environment protects the records in the Readout Application against tampering.

Failure to correctly transfer audit records between Readout Application and Register (VII)	
VII.1: Modification of audit records in transit between Readout Application to Register. This includes: □ Accidental modification (e.g. transmission errors) □ Sending an invalid or truncated set of audit records □ Deliberate modification	If the TOE is a Class B1 TOE, this threat is not relevant. If the TOE is not a class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications and a means for sender authentication. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed
VII.2: Deletion of audit records in transit between Readout Application to Register	If the TOE is a Class B1 TOE, this threat is not relevant. If the TOE is not a class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed.
VII.3: Insertion of audit records in transit between Readout Application to Register. This includes: □ Audit records being sent twice (either deliberately or by accident) □ Unauthenticated or unknown parties sending audit records	If the TOE is a Class B1 TOE, this threat is not relevant. If the TOE is not a class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all insertions and a means for sender authentication. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed.
VII.4: Reading of audit records in transit between Readout Application to Register	If the TOE is a Class B1 TOE, this threat is not relevant. If the TOE is not a class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the events while in transit. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed. O.SEND_TO_CORRECT_PARTY additionally ensures that the audit records will only be sent to the Register, further decreasing the risk of this threat.
Failure to correctly register records at the Register (VIII)	
VIII.1 Modification of audit records while at the Register. This includes: □ Accidental modification (e.g. storage, processing or conversion errors) □ Deliberate modification	OE.REGISTER_PROTECT_RECORDS specifies that modifications are prevented.

VIII.2 Deletion of audit records while at the Register	OE.REGISTER_PROTECT_RECORDS specifies that deletion is prevented.
VIII.3 Insertion of audit records while at the Register	OE.REGISTER_PROTECT_RECORDS specifies that insertion is prevented.
VIII.4 Reading of audit records while at the Register	OE.REGISTER_PROTECT_RECORDS specifies that the reading of records is prevented.
Failure to correctly transfer audit records between Readout Application and Broker (IX)	
IX.1: Modification of audit records in transit between Readout Application to Broker. This includes: □ Accidental modification (e.g. transmission errors) □ Sending an invalid or truncated set of audit records □ Deliberate modification	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications and a means for sender authentication. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed. If the TOE is a Class B2 TOE, OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for Class B2 TOEs, the records are protected between Broker and Readout Application.
IX.2: Deletion of audit records in transit between Readout Application to Broker	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed. If the TOE is a Class B2 TOE, OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for Class B2 TOEs, the records are protected between Broker and Readout Application.
IX.3: Insertion of audit records in transit between Readout Application to Broker. This includes: □ Audit records being sent twice (either deliberately or by accident) □ Unauthenticated or unknown parties sending audit records	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all insertions and a means for sender authentication. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed. If the TOE is a Class B2 TOE, OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for Class B2 TOEs, the records are protected between Broker and Readout Application.

IX.4: Reading of audit records in transit between Readout Application to Broker. This includes: □ Audit records being sent by the Readout Application to the wrong Broker □ Audit records being sent by the Broker to the wrong Readout Application	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the events while in transit. Note that in the case of transparent Readout Applications, this means may rely on the original encryption of the audit records, and this is explicitly allowed. O.SEND_TO_CORRECT_PARTY additionally ensures that the audit records will only be sent to the correct Broker, further decreasing the risk of this threat. If the TOE is a Class B2 TOE, OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for Class B2 TOEs, the records are protected between Broker and Readout Application, and that they are sent to the correct Readout Application.
Failure to correctly convert records at the Broker (X)	
X.1 Modification of audit records while at the Broker. This includes: □ Accidental modification (e.g. storage, processing or conversion errors) □ Deliberate modification	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_RECORDS specifies that modifications are prevented. OE.BROKER_CORRECT_CONVERSION specifies additionally that the conversion process is accurate.
X.2 Deletion of audit records while at the Broker	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_RECORDS specifies that deletion is prevented.
X.3 Insertion of audit records while at the Broker	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_RECORDS specifies that insertion is prevented.
X.4 Reading of audit records while at the Broker	If the TOE is not a Class B TOE, this threat is not relevant. If the TOE is a Class B TOE: OE.BROKER_PROTECT_RECORDS specifies that the reading of records is prevented, and also specifies secure deletion once the records have been transferred to the Register, thus further reducing the risk of unauthorized reading.

Failure to correctly transfer audit records between Broker and Register (XI)	
XI.1: Modification of audit records in transit between Broker and the Register. This includes: □ Accidental modification (e.g. transmission errors) □ Deliberate modification	If the TOE is not a Class B1 TOE, this threat is not relevant. If the TOE is a Class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications.
XI.2: Deletion of audit records in transit between Broker and Register.	If the TOE is not a Class B1 TOE, this threat is not relevant. If the TOE is a Class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions.
XI.3: Insertion of audit records in transit between Broker and Register. This includes: □ Audit records being sent twice (either deliberately or by accident) □ Unauthenticated or unknown parties sending audit records	If the TOE is not a Class B1 TOE, this threat is not relevant. If the TOE is a Class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all insertions and a method for sender authentication.
XI.4: Reading of audit records in transit between Broker and Register	If the TOE is not a Class B1 TOE, this threat is not relevant. If the TOE is a Class B1 TOE: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the events while in transit. OE.BROKER_SEND_TO_CORRECT_PARTY additionally ensures that the audit records will only be sent to the Register, further decreasing the risk of this threat.

6.2 Security Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.DETECT_EVENTS The combination of Handset and OBU shall detect all events required by the applicable laws and regulations.	This objective is met by: □ FAU_GEN.1 specifying that audit events must be generated from the events (and that they must therefore be detected. The application note under the SFR specifies that completion of the SFR must conform to the applicable laws and regulations. □ FPT_STM.1 specifying that the TOE must contain a reliable clock, to be able to store date and time of an event.
O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_OBU The Handset and OBU shall protect information about detected events as this is exchanged between them against insertion, deletion and modification.	This objective is met by FDP_ITT.3, which restates the objective and additionally specifies the action to be taken when this occurs. .
O.RECORD_AND_ENCRYPT_EVENTS_IN_OBU The OBU shall store all required information for each event in audit records in the OBU. Each audit record shall contain at least: □ The information required by the applicable laws and regulations. □ A unique consecutive number for each audit record. The OBU shall store all audit records in such a way that they cannot be read or modified by unauthorized entities. The OBU shall encrypt all audit records before allowing them to be read out in such a way that they cannot be read or modified by unauthorized entities.	This objective is met by: □ FAU_GEN.1 and its Application Note that specify that the audit records must contain the information required by the applicable laws and regulations. □ FAU_STG.1 specifying that they must be stored in such away that they cannot be modified (or deleted) or read by unauthorized entities. □ FCS_COP.1(1) specifying that the audit records must be encrypted before sending (and therefore cannot be read by unauthorized entities) □ FDP_ITT.1 further specifying that the records cannot be modified and or disclosed by unauthrorised entities when they are read out
O.TAMPER_EVIDENT_HANDSET_AND_OBU The Handset and OBU shall be tamper-evident. Evidence of tampering does not have to be detectable in the field, but shall be detectable under close scrutiny of an expert.	This objective is met by FPT_PHP.1(1) which, together with the Application Note restates the objective.
O.TAMPER_EVIDENT_READOUT_APPLICATION (Only for Class C1 TOEs) The Readout Application shall be tamper-evident. Evidence of tampering does not have to be detectable in the field, but shall be detectable under close scrutiny of an expert.	This objective is met by FPT_PHP.1(2) which, together with the Application Note restates the objective. The footnote indicates that the SFR is only valid for Class C1 TOEs.

Security objectives	SFRs addressing the security objectives
O.NO_OVERFLOW_IN_OBU When the memory of the OBU is filled with audit records for: □ 90%, the OBU shall issue an early recall warning to the driver □ 100%, the OBU shall no longer allow the car to start	This objective is met by: □ FAU_STG.3 which restates the first bullet □ FAU_STG.4 which restates the second bullet
O.OBU_AND_READOUT_APPLICATION The OBU shall allow only the Readout Application to: □ Read out audit records from the OBU □ Delete audit records from the OBU □ Calibrate the OBU and the Handset	This objective is met by FDP_ACC.1 and FDP_ACF.1. The rules in ACF.1 restate the objective.
O.READOUT_APPLICATION_AUTHENTICATION Before a human user can use the Readout Application, this user must first be identified and authenticated.	If I&A is done by the TOE, this objective is met by FIA_UID.2 and FIA_UAU.2, which restate the objective. If I&A is done by the operational environment, this objective is automatically met
O.READOUT_APPLICATION_PROTECT_RECORDS The Readout Application shall not allow its users (or other entities) to insert, modify or read audit records from the Readout Application. This includes reading of audit records after they have been sent onwards.	This objective is met by FDP_ACC.1 and FDP_ACF.1, which strictly limit the operations that Readout Application can do. Additionally, for C1 and C2 TOEs (which decrypt the audit records), FDP_RIP.1 guarantees that the audit records are securely deleted. For other TOEs, the audit records are never available in the clear, so this is unnecessary. The C1 and C2 TOEs must also decrypt and re-encrypt the records to protect them, so FCS_COP.1(2) and FCS_COP1(3) also support this objective.
O.SEND_TO_CORRECT_PARTY The Readout Application shall send the audit records only to the correct party in the correct manner. The Readout Application shall be able to receive a confirmation that the audit records have been correctly received. □ For Class B1 TOEs, the audit records shall be sent to the Broker, using the method specified by the Broker, and the confirmation will be received from the Broker □ For Class B2 TOEs, the audit records shall be sent to the Broker, using the method specified by the Broker, then the records received by the Broker shall be sent to the Register, using the method specified by the Register, and the conformation shall be received from the Register. □ For all other Classes of TOEs, the audit records shall be sent to the Register, using the method specified by the Register, and the confirmation will be received from the Register.	This objective is met by FDP_ACC.1 and FDP_ACF.1: □ that specify that for class B1 TOEs the Readout Application can only send the audit records to the Broker in the manner specified by the Broker □ that specify that for Class B2 TOEs the Readout Application sends the records to the Broker in the manner specified by the Broker, that receives new records in return from the Broker and then sends them to the Register in the manner specified by the Register □ that specify that for class A and C TOEs the Readout Application can only send to the audit records to the Register in the manner specified by the Register □ that specify that for Class B1 TOEs the confirmation is received from the Broker □ that specify that for Class A, B2 and C TOEs the confirmation is received from the Register

6.3 Dependencies

SFR	Dependencies
FAU_GEN.1	FPT_STM.1: Met
FAU_STG.1	FAU_GEN.1: Met
FAU_STG.3	FAU_STG.1: Met
FAU_STG.4	FAU_STG.1: Met FAU_STG.3: Met
FCS_COP.1(1)	[FDP_ITC or FDP_ITC.2 or FCS_CKM.1]: Not met. See section 5.3 for details. FCS_CKM.4: Not met. See section 5.3 for details.
FCS_COP.1(2)	[FDP_ITC or FDP_ITC.2 or FCS_CKM.1]: Not met. See section 5.3 for details. FCS_CKM.4: Not met. See section 5.3 for details.
FCS_COP.1(3)	[FDP_ITC or FDP_ITC.2 or FCS_CKM.1]: Not met. See section 5.3 for details. FCS_CKM.4: Not met. See section 5.3 for details.
FDP_ACC.1	FDP_ACF.1: Met
FDP_ACF.1	FDP_ACC.1: Met FMT_MSA.3: Unnecessary, since there are no security attributes
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1: Met by FDP_ACC.1
FDP_ITT.3	FDP_ACC.1 or FDP_IFC.1: Unnecessary, since the reference to the policy was refined away. There exists an Access Control policy in this PP, but this does not concern the communication between Handset and OBU and is therefore irrelevant to this SFR. FDP_ITT.1: Unnecessary, as it is not required for the TOE to prevent modification/loss of use on the connection between Handset and OBU: it needs only to detect this and then take action. There is an FDP_ITT.1 SFR included in the PP but this is not related to this FDP_ITT.3 SFR and therefore is unrelated to this dependency.
FDP_RIP.1	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	-
FPT_PHP.1(1)	-
FPT_PHP.1(2)	-
FPT_STM.1	-
EAL3	All dependencies within an EAL are satisfied
ALC_FLR.2	-