Note: This annex has been removed from later versions of draft TS 17575

Annex C
(informative)

Compliance checking provisions

C.1 Introduction

This annex provides an overview of provisions for compliance checking i.e. for the process of compelling observance of a toll regime. As shown, the event handling provisions (see Clause 5) can be easily used to support compliance checking as well.

Although parts of this annex are not directly related to the OBE update provisions, they are still indirectly relevant insofar a user should be able to describe the use of these compliance checking provisions in an OBE instruction module as defined in this part of TS 17575.

Compliance checking measures are an essential part of tolling services. In this Annex the focus is on enforceability, on the possibilities to detect non-compliant behaviour or other violations of the toll regime. Procedures for tracking down the one(s) liable for toll, for settlement, for prosecution, and for the execution of verdicts are outside the scope of this Technical Specification.

With respect to the detection of non-complaint behaviour the following types of measures can be distinguished:

a) Unobtrusive surveillance,
i.e. not noticeable for the OBE, e.g. with video techniques, in which case the toll declarations from the vehicle can be checked afterwards on their consistence with presence of the vehicle as observed by a video camera.

NOTE 1 The use of video cameras in unobtrusive surveillance requires that the vehicle's registration number is included in the toll declarations.

b) OBE interrogating with on the spot checks
by interrogating the OBE and checking the validity of the response on the spot.

NOTE 2 In case of a DSRC based toll system, the validity of the toll declaration itself is checked. In case of a GNSS based system the OBE is interrogated with dedicated compliance checking transactions. Only the latter are within the scope of this Technical Specification.

c) OBE interrogating with checks afterwards
in which case the response of the OBE is checked afterwards on its consistency with the toll declarations received by the toll system.

NOTE 3 In this case one can also check whether or not the data received in a compliance checking transaction was also used for the determination of the toll. I.e., if one has to reckon with the possibility that the OBE might lie when interrogated. So also simply asking whether or not the OBE 'feels well' or has successfully completed a self test is of little value unless, perhaps, an incorrect response can be used to proof forgery.

NOTE 4 On the other hand, as the OBE is aware of the interrogation, it might only 'lie' when it has not been interrogated.

The dilemma presented in the previous paragraph can be avoided by securely monitoring the fee determination and declaration process in the OBE.

NOTE 5 Although the basic principles and compliance checking provisions can be equally applied to other application as well, this annex is written for toll collection. For a more general understanding, one should read 'main module provider'

for 'toll service' provider. The OBE instruction module may be issued by either the toll charger or the toll service provider depending on contractual the context.

C.2 Basic principles

C.2.1 Valid toll declarations

The basic concept is that a 'valid toll declaration' provides a toll charger with a valid and undisputable claim for the fee on a toll service provider and/or its customer.

Depending on contractual arrangements outside the scope of this Technical Specification, a valid toll declaration may be issued by the OBE or by the toll service provider. In the latter case the OBE only provides raw data that is used by the toll service provider to make the toll declaration.

Note that a 'valid toll declaration' only implies that the responsibility for the content is clear, not that the data is correct. Valid data may be incorrect.

EXAMPLE A properly signed message may still contain incorrect data. E.g., the number of axles or the presence of a trailer may be incorrect. Such a toll declaration provides the toll charger with a wrong but valid claim.

Valid but incorrect toll declarations must be detectable with appropriate compliance checking measures.

The moment a toll system regards the communication with the OBE as correct and valid, can be seen as the moment that a toll agreement is concluded or as the moment that the one(s) liable for toll fulfilled their toll declaration responsibilities.

The concept of a 'valid toll declaration' is the 'linking pin' between:

a) the equipment interoperability and the organisational interoperability,

b) the toll service provider and the toll charger, and

c) the charging and compliance checking measures and procedures.

NOTE When the toll charger does not receive a valid declaration the vehicle should be regarded as non-equipped vehicle, the appropriate local compliance checking measures should be applied and the toll charger should collect the fee and a possible fine from the one(s) liable for toll according to the local toll regime (who may not be the same as the customer of the toll service provider). This, however, is outside the scope of this Technical Specification.

C.2.2 Compliance checking support

Compliance checking as set out in this Annex is based on the idea that the onboard process of producing toll declarations can be 'securely' monitored in the sense that:

a) a log of records can be created

b) the log records contain enough data to draw conclusions about a correct functioning of the OBE

c) the toll declarations send to the toll charger can be calculated from or are the same as the log records.

d) the validity and correctness of the most recent records can be checked on the spot

e) any change of a logged record afterwards can be detected

f) the log is owned by the toll service provider but the a toll charge may request a copy.

C.3 Overview of the onboard provisions

As this Technical Specification is dealing with the communication with the OBE, the following description of onboard provisions is not binding for an implementer. Nevertheless it provides some insight on how the security provision could be implemented.

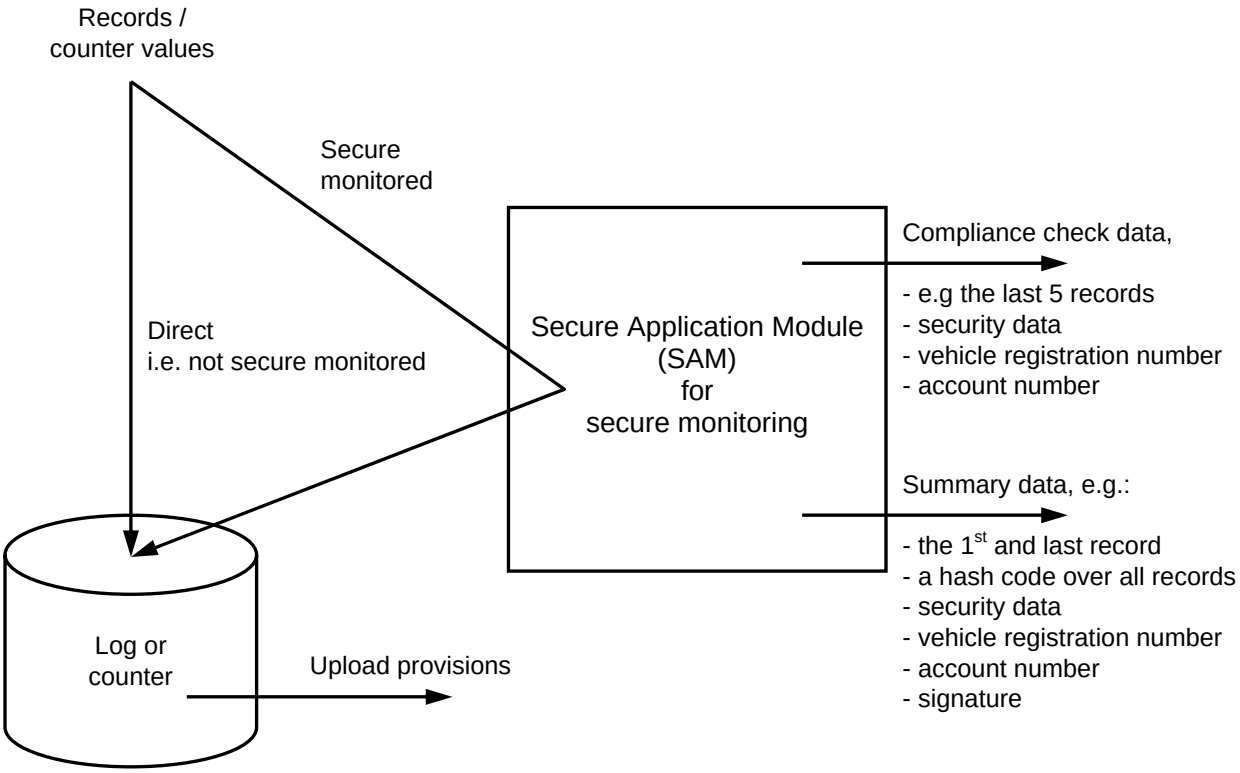

Figure C.1 — Secure monitoring of a record list or counter

The figure above shows the difference between direct logging and a secure monitored log. In the latter case all log records pass a Secure Application Module (SAM) which calculates an hash-code over the stream of log records and performs some elementary checks (see below).

NOTE The Secure Application Module (SAM), may be e.g. a small size smart card with secure monitoring as a secure application.

Note that the toll charger has to trust the functioning of the SAM. This may be accomplished by security provisions when the SAM is manufactured and initialised as a 'secure monitoring card for tolling'. The latter may be accomplished by requiring that a trusted third party is doing this initialisation before the SAM is handed over to a toll service provider for further personalisation. This trusted third party may write the card's private signature key into the card, and may issue a certificate with the public verification key. Such measures are, however, out of scope of this Technical Specification.

Note also that the toll service provider should be responsible for retaining the monitored log. The right of the toll charger to have a copy of a monitored log may be bound to suspicious situations and/or a certain number of random checks. If a log cannot be shown to the toll charger the burden of proof for the correctness of the toll declaration may be shifted to the toll service provider and/or its customer. These measures are, however, also out of the scope of this Technical Specification.

NOTE Also, provision to make the log available to the customer of a toll service provider, i.e. for accounting purposes, are outside the scope of this Technical Specification.

For a proper functioning the toll service provider has to personalise the SAM with the vehicle's registration number and the account number of the user. The vehicle's registration number is needed in a compliance

checking record in order to show that the record is indeed from the vehicle with that registration number. The account number is needed to relate signed data to an account.

C.4 Additional event handling requirements

C.4.1 Introduction

Clause 5 specifies a mechanism for event handling. As already indicated above, this mechanism can be used with a few simple extensions for secure monitoring too.

If used for secure monitoring the party who wants to monitor the behaviour of the OBE only has to specify when (i.e. for which events under which conditions) the OBE has to generate a record for a record list or to increment a counter and instruct the OBE that the production of those records and counter increment records shall be securely monitored.

This requires provisions (see the next subclauses for details)

a) to indicate that a record list or counter shall be securely monitored,

b) to summarize and store a log of securely monitored records or counter increments together with its associated security data,

c) to include in the summary the results of checks performed on the sequence of counter values or log records,

d) to include in the summary a record which signals detected attempts to tamper the SAM, and

e) to upload the data and control its removal.

C.4.2 Security extensions to the definition of a record list or counter

A generic mechanism to create a record list or a counter is specified in subclauses 5.2.5 and 5.2.6. Both can be securely monitored if the number of (counter) records[1] that shall be securely retained (for use in a compliance checking transaction) is added to the definition of the record list or counter.

It is up to the implementer to assure that the records of counter values are securely monitored.

C.4.3 Summarizing a list of counter values and/of log records

On a certain moment one must be able to draw up the result of a monitoring period and to produce a summary record that reflects the results and allows for an undisputable detection of any changes that haven been made afterwards in this monitored log.

Then, a summary record shall contain the following data:

a) The secure log identifier, a sequence number assigned by the SAM to identify the monitored log among all other logs monitored by this SAM.

b) The account number of the customer (which should also identify the toll service provider)

c) The vehicle's registration number

d) The date-time when the summary was produced

---

[1] The term counter record is used for a record that describes a counter increment.

e) The first and last (counter) record
To show that a sequence of summary records is complete and, in case of counter values these first and last values may also contain sufficient information to calculate a fee due.

f) The hash code over the log, i.e. the monitored records or counter records

g) An identification of the hashing algorithm that has been used.

h) A summary of the checks that have been performed (see below)

i) A summary of events that may indicate attempts to tamper the SAM (see below)

j) A signature over the data listed above on behalf of the toll service provider as the party responsible for a correct functioning of the OBE

k) An identification of the hashing and signature algorithm used for the signature

Both the account number and the vehicle's registration number are assumed to be added to the SAM during personalisation. The identifiers for the hashing and signature algorithms already be added at the production stage.

In order to summarise a monitoring period a summarizing action with the argument has been defined.

a) An indication whether the monitoring process has to be resumed or ended

b) If the secure monitoring has to be resumed, whether the last record has to become the first one for the next period, or not.

Due to the very nature of this action, both the fixed and random delay parameters should be set to zero when this action is used in an OBE instructions module.

C.4.4 Security data: records checking

As monitored records contain both location and time, some very elementary checks can be performed:

a) The minimum and maximum elapsed time between monitored (counter) records can be reported
Note that the production time of a (counter) record should be recorded in this record. A SAM might be a small size smart card and might not have a clock.

b) The time as recorded in the monitored (counter) records must be increasing
(note that)

c) The minimum and maximum distance between recorded vehicle locations.

d) The minimum and maximum speed based on the distance between vehicle locations.

And in case counter values are monitored the minimum and maximum increments can be monitored as well.

In case a summary record contains a suspicious value one can inspect the whole log.

C.4.5 Security data: tampering indications

The following parameters can be used, if supported by the hardware, to indicate a possible tampering attempt:

a) high and low voltage detection

b) high and low clock frequency detection

c) high and low temperature detection

Whether or not monitoring of these parameters shall be implemented shall be agreed between the toll charger and the toll service provider and is out of the scope of this Technical Specification. This Technical Specification only specifies the provisions for the exchange of these parameters.

C.4.6 Uploading monitored data and controlling its removal

TEMP NOTE This subclause has to be tuned to the part(s) in which the transaction(s) will to defined (e.g. a compliance checking part).

Although upload transactions are outside the scope of this part of DTS 17575 which deals with downloads, any parameters required to control uploads and subsequent deletion of securely monitored monitored logs must be included in an instruction module and are therefore within the scope of this part of DTS 17575.

With respect to the upload and/or deletion of monitored logs from OBE, the following has to be considered:

a) A monitored log primarily serves the interest of the toll service provider and, once produced, should be 'owned' by the toll service provider. Consequently. the toll service provider should be the only party able to delete a monitored log from the OBE.

   If a monitored log is lost, the burden of proof that the OBE was functioning correct is at the toll service provider. Consequently, the purpose of the log is to prove that the OBE was functioning correct.

   Depending on the relation between the toll service provider and a toll charger the instruction module for securely monitored record lists and counters may be issued by the toll service provider, toll charger or a third party. In either case it is assumed that the OBE is instructed to produce a monitored log with sufficient information for the toll service provider to show that his OBE was functioning correctly.

b) A toll charger shall be allowed to have access to a monitored log in order to check whether the OBE was functioning correctly or not. However as a change of a monitored log can be detected afterwards, there are no real-time requirements and it is immaterial from which source a toll charger shall have to obtains this monitored log. This may be directly form the OBE, from the central equipment of the toll service provider or from any third party. Details can be arranged e.g. contractually but are outside the scope of this Technical Specification.

c) This Technical Specification may allow a toll charger to instruct the OBE to upload a monitored log.

   More formally, this Technical Specification allows the issuer of an OBE instruction module to instruct the OBE to upload a monitored log to himself or to any third party.

d) A toll service provider may use any means for uploading monitored logs, e.g. an USB / infrared / Bluetooth etc, connection to a laptop or some device connected to his central equipment. However, these kind of provisions are outside the scope of this Technical Specification.

In order to fulfil these requirements the following has been defined (see Clause 5):

a) An action to upload the most recently summarised list of (counter) records. The event to trigger this action should occur while the vehicle is still in the use domain of the OBE instruction module.

b) an attribute for the number of summary records and associated monitored logs in the OBE.
   A change of the value attribute can be used as an event to trigger e.g. an instruction to upload and delete the monitored log and its summary from the OBE.

c) an action to invoke an upload transaction for monitored logs and their summary to the toll service provider. This action will be performed only if included in an instruction module issued by the toll service provider. After a successful upload, the monitored log will be deleted from the OBE.

C.5 Compliance checking transactions

C.5.1 Introduction

TEMP NOTE This subclause may be tuned or moved to. a compliance checking part.

Although compliance checking transactions are outside the scope of this part of DTS 17575, the implications of those transactions for the data to be downloaded into the OBE should be known and included.

C.5.2 Service description

With respect to DSRC compliance checking transactions, the following has to be considered:

a) A toll charger should be able to use compliance checking transactions on the spot at random locations and, preferably, also from mobiles.

b) A toll domain may encompass multiple tolled objects for which one or more tariff schemes may apply. However a compliance checking transaction should only check current or rather recent OBE behaviour. Consequently and in order to be able to perform a compliance checking transaction in due time, a toll charger should be able to limit the number of securely monitored logs or counter to be checked in a compliance checking transaction. This may be accomplished in several ways:

   1) Do not use more securely monitored logs or counters then strictly necessarily. This is the responsibility of the user when defining the OBE instruction module.

   2) Allow the compliance checking equipment to select the securely monitored logs or counters.

   3) Support an action that may suspend checking a log or a counter when there is no need for it. << for further study >>

      EXAMPLE In one toll domain (country) a toll may be levied for urban zones and the toll charger may only want to use one counter for this toll that will be summarized once a month. A similar situation may apply for the interurban motorways. In such a case it makes sense to suspend checking the counter for the urban toll on motorways and for the motorway toll on local roads.

   Nevertheless, it should be noted that a standard can and should not stipulate that it must be used in a prudent and efficient way. That is the sole responsibility of its users. A standard can only facilitate efficient use.

c) A compliance checking transaction can be used to identify a vehicle and should therefore adhere to local privacy and security regulations.

   TEMP NOTE For further study, we may look to the ERI standard that had to cope with a similar situation. As for ERI the OBE may support readers with various capability levels.

Consequently and apart from confidentiality provisions, the result of a compliance checking transaction should contain:

a) the few last records or counter values of the relevant logs or counters

b) per log or counter, the result of the security checks (as to be used for the summary record)

c) the indications of possible tampering of the SAM (as also used for a summary record)

d) a signature on behalf of the toll service provider over these values.

NOTE Fraud prevention requires that the OBE shall not be able to register correct values when checked and incorrect values when not. In order to prevent this one may make the time required to write the values to be checked into the SAM significant longer than the time needed for a compliance checking transaction.

A DSRC transaction can be used for interrogating the OBE with on the spot checks. For checks afterwards a DSRC transaction may only instruct the OBE to invoke a transaction for sending the compliance checking data to some central equipment. In the later case there are less stringent time constraints.

C.5.3 Protocol description

TEMP NOTE This subclause may be moved to a part or standard for compliance checking.

C.5.3.1 The compliance check transaction

C.5.3.1.1 Invocation and perfomance

The compliance check transaction shall be used to check whether the behaviour of the OBE complies with the requirements of a toll regimen (as specified in an instruction module).

The compliance check transaction shall be invoked by:

a) Compliance checking equipment outside the vehicle, e.g. roadside or mobile equipment and then performed by the OBE, or,

b) in case the SAM is not integrated in the DSRC unit of the OBE, by the OBE and then performed by the SAM.

C.5.3.1.2 The complianceCheck transaction definition

The complianceCheck transaction is defined as follows.

```
complianceCheck TRANSACTION ::= {
        ARGUMENT                ComplianceCheckArgument
        RESULT                  SignedSpotCheckData
        ERRORS                  {ComplianceCheckErrors}
        CODE                    3
        }
```

The complianceCheck transaction is ivoked with an argument the ComplinaceCheckArgument type as specified below.

If the transaction is performed successfully a result of the SignedSpotCheckData type is returned. If not, one of the error codes from ComplianceCheckErrors is returned.

C.5.3.1.3 The argument of the complianceCheck transaction

The type is used for the argument of the complianceCheck transaction and is defined as follows.

```
ComplianceCheckArgument ::= SEQUENCE {
        recordListIds           SEQUENCE OF ObjectId OPTIONAL,
        counterIds              SEQUENCE OF ObjectId OPTIONAL
        }
```

The recordListIds component, if present, shall be used to identify the record lists for which the retained records are to be returned in the result of the transactions.

If present, only the retained records of the identified record lists, if currently securely monitored, are to be returned in the result.

The record list identifier used is the one as assigned to the list in its record list definition in the OBE instruction module.

If absent, the retained records of all currently securely monitored record lists are to be returned in the result.

The counterIds component, if present, shall be used to identify the counters for which the retained counter records are to be returned in the result of the transactions.

If present, only the retained counter records of the identified counters, if currently securely monitored, are to be returned in the result.

The counter identifier used is the one as assigned to the counter in the counter definition in the OBE instruction module.

If absent, the retained counter records of all currently securely monitored counters are to be returned in the result.

NOTE 1 It not regarded to be error when the argument contains identifiers that are not in use by the OBE. This property may be used to deal with e.g. different versions of the OBE instruction module.

NOTE 2 If no retained (counter) records should be returned at all, the argument should contain both a unused record list number and an unused counter number.

C.5.3.1.4 Error of the complianceCheck transaction errors

The type specifies the supported error codes for the compliance check transaction and is defined as follows.

```
ComplianceCheckErrors INTEGER ::= {invalidArgument}
```

The invalidArgument code is used to signal any error in the transaction's argument.

C.5.3.2 The use of the DRSC for the communication with mobiles or road side equipment

TEMP NOTE This section has to be tuned with ISO 15509 !!!

C.5.3.2.1 General

An secure monitoring (SM) application layer protocol data unit to be exchanged between a SAM and the OBE or between the OBE and mobile or road side compliance checking equipment shall be a SM protocol data unit of type EFC-SM-PDU, i.e. of type SMRequestPdu or of type SMResponsePdu.

A SM protocol data unit shall be encoded in conformance with to the canonical Packed Encoding Rules (CANONICAL-PER) ALIGNED variant defined in ISO/IEC 8825-2.

If the DSRC application layer protocol is used for SM transactions, ISO 15628 (or EN 12834 within the EU) shall be applied as specified in this clause.

NOTE This makes the DSRC interface for SM transactions compatible with other DSRC application interfaces such as ISO 14906.

C.5.3.2.2 Use of the DSRC initialization service

Whenever a DSRC link is to be used for SM transactions, the ISO 15628 / EN 12834 initialization service shall be used as follows:

— Either the mandApplications component or the nonmandApplications component of the initialisation-request T-PDU (Beacon Service Table, BST) shall contain an EFC application component.

— The applications component of the initialisation-response T-PDU (Vehicle Service Table, VST) shall contain an EFC application component.

— The value of the EFC application component in an initialisation-request or an initialisation-response shall be as follows:

— The aid component shall have the value “electronic-fee-collection”.

— The eid component may be omitted and, if present, shall be ignored by the SM transactions.

— The parameter component may be omitted and, if present, shall be ignored by the SM transactions.

NOTE 1 The designation of an application as mandatory or non-mandatory and its position in the list of applications is outside the scope of this part of ISO/TS 17575. It only influences the priority of the SM transactions relative to other applications identified in the BST (see 7.3.2.2 of ISO 15628 or 7.3.2 of EN 12834).

NOTE 2 The eid component and the parameter component may however be used for other, non-MS transaction in EFC applications.

C.5.3.2.3 Use of the DSRC action request

A SM transaction request is sent from the compliance checking equipment to the onboard DSRC unit as an ISO 15628 / EN 12834 action-request as follows:

— The value of the mode component shall be TRUE (as all MS transactions are confirmed).

— The value of the eid component shall be 0.

— The value of the actionType component shall be smTransaction << to be registered with NEN >>.

— The accessCredentials component shall not be present.

— The value of the accessParameter component shall be passed as received to the SAM as the value of an SMRequestPdu.

— The iid component shall not be present.

NOTE The action-request is of type Action-Request which is defined in ISO 15628 / EN 12834 as follows:

```
Action-Request::=SEQUENCE{
        mode                    BOOLEAN,
        eid                     Dsrc-EID,
        action                  Type ActionType,
        accessCredentials       OCTET STRING (SIZE (0..127,...)) OPTIONAL,
        actionParameter         Container OPTIONAL,
        iid                     Dsrc-EID OPTIONAL
        }
```

(end of note)

C.5.3.2.4 Use of the DSRC action response

An MS transaction response received from an SAM is sent by the onboard DSRC unit to the compliance checking equipment as an ISO 15628 / EN 12834 action-response as follows:

— The value of the eid component shall be 0.

— The iid component shall not be present.

— The value of the responseParameter component, if present, shall be the value of the MSResponsePdu as received from the SAM.

— The ret component may be omitted and, if present, shall be ignored when the MSResponsePdu is also present.

NOTE 1 The action-response shall be of type Action-Response which is defined in ISO 15628 / EN 12834 as follows:

```
Action-Response::=SEQUENCE{
        Fill                    BIT STRING (SIZE(1)),
        eid                     Dsrc-EID,
        iid                     Dsrc-EID OPTIONAL,
        responseParameter       Container OPTIONAL,
        ret                     ReturnStatus OPTIONAL
        }
```

(end of note)

In case the DSRC device is not capable of transferring an SMRequestPdu to the SAM, an ISO 15628 / EN 12834 action-response containing a ret component of type ReturnStatus is returned to the compliance checking equipment.

NOTE 2 The mechanisms to be used for passing an MSRequestPdu from a DSRC device to the SAM are outside the scope of this part of ISO/TS 17575. It is assumed that some generic onboard platform or network will emerge that can be used for this purpose. In the meantime, the manufacturer of a DSRC device may have to cope with different means for connecting its DSRC device to onboard reader/writer of the SAM.

C.5.3.2.5 Embedding of SM transactions in the DSRC application layer definition

See the ASN.1 module 'Reduced ISO 15628 MODULE' below.

C.6 The communication with the secure monitoring SAM

TEMP NOTE This section might be moved with a more precise specification to a compliance checking part.

C.6.1 Overview

The interface with the SAM is outside the scope of this part or TS 17575. However in order to provide the service it should support:

a) personalisation of the SAM for a particular vehicle and account,

b) See annex B for the data needed for the personalisation of the SAM.

c) monitoring a (counter) record, (see below)

d) compliance checking transactions, and

e) the production of a summary record (with a sequence number assigned by the SAM).

C.6.2 Monitoring a (counter) record

The monitor record transaction shall be invoked whenever:

a) .a 'log record' or 'increment counter' action (see 5.2.4.5.2) has to be performed for a securely monitored record list or counter; or

b) an empty record list or reset counter action has to be performed on a non-empty securely monitored record list or counter (see 5.2.5.5.2and 5.2.6.6.2 for details)

c) a summarise record list or summarise counter action has to be perform for non empty monitored log with the leaveLastRecordAnd Continue parameter (see 5.2.5.5.2and 5.2.6.6.2 for details).

A compliance checking part might define the SAM transaction for monitoring a (counter) record as follows.

```
monitorRecord TRANSACTION ::= {
        ARGUMENT                MonitorRecordArgument
        RESULT                  ObjectId
        ERRORS                  {MonitorRecordErrors}
        CODE                    5
        }

MonitorRecordArgument ::= SEQUENCE {
        secureLogId             ObjectId OPTIONAL,          -- absent for a new log
        record                  MonitoredRecord
        }

MonitorRecordErrors INTEGER ::= {invalidArgument}
```

The argument should identify the securely monitored log and contain the (counter) record to be monitored.

The result should contain the identifier for the securely monitored log (at least required when the first (counter) record has been written into the log.

C.6.3 Creating a summary

A compliance checking part might define the SAM transaction for monitoring a (counter) record as follows.

```
summariseLog TRANSACTION ::= {
        ARGUMENT                SummariseLogArgument
        RESULT                  SignedSummary
        ERRORS                  {SummariseLogErrors}
        CODE                    4
        }

SummariseLogArgument ::= SEQUENCE {
        secureLogId             ObjectId,
        summarisationTime       DateTimeAndDiff
        }

SummariseLogErrors INTEGER ::= {invalidArgument}
```

The argument should identify the log and provide the day and time.

The result should contain the summary signed by the SAM.

C.6.4 The use of the lower layers

An secure monitoring (SM) application layer protocol data unit to be exchanged between a SAM and the OBE or between the OBE and mobile or road side compliance checking equipment shall be a SM protocol data unit of type EFC-SM-PDU, i.e. of type SMRequestPdu or of type SMResponsePdu.

A SM protocol data unit shall be encoded in conformance with to the canonical Packed Encoding Rules (CANONICAL-PER) ALIGNED variant defined in ISO/IEC 8825-2.

NOTE If required, an SM protocol data unit may be segmented and reassembled (in ISO/IEC 7498-1 terminology) as appropriate.

C.6.5 The use of an ISO 14443 inteface for the SAM

In the case where the interface between a SAM and the other OBE is based on ISO/IEC 14443, applies and the interface shall comply with ISO/IEC 14443 part 1, 2, 3, and 4, and with:

— the SAM acting as a PICC (Proximity Integrated Circuit card) of type A or B;

— the other OBE acting as a PCD (Proximity Coupling Device) supporting both types A and B.

An SM protocol data unit shall be directly transferred using the INF field of one or more I-blocks (see ISO/IEC 14443-4).

NOTE 1 Consequently, an SM protocol data unit is not packed into ISO/IEC 7816-4 application protocol data units as suggested in ISO/IEC 14443-4.

Segmenting and reassembling of an SM protocol data unit shall be accomplished, if required, with chaining as specified in ISO/IEC 14443-4.

The SAM data can only be accessed as specified in this part of ISO/TS 17572 << to be changed >>.

C.7 ASN.1 modules for secure monitoring (and compliance checking)

C.7.1 The SM transaction module

```
SecureMonitoringTransactionsModule
{iso(1) standard(0) iso17575(17575) part2 (2) secureMonitoringTransactions (13) version (0)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

-- Secure montitoring transactions

-- EXPORTS  everything;

IMPORTS
        TRANSACTION, EntityId           FROM EfcPart4Modules     -- to be replaces by the actual part 4 module(s)
        ObjectId, DateTimeAndDiff       FROM ObeInstructionsHandlingModule
        MonitoredRecord, SignedSpotCheckData, SignedSummary
                                        FROM RecordsAndCountersModule
;

--Secure monitoring PDU's

EFC-SM-PDU ::= CHOICE {
        requestPdu                      SMRequestPdu,
        responsePdu                     SMResponsePdu
        }

SMRequestPdu ::= SEQUENCE {
        invokeId                        INTEGER,
        transactCode                    TRANSACTION.&transactionCode ({EFC-SM-Transactions }),
        argument                        TRANSACTION.&ArgumentType ({EFC-SM-Transactions} {@transactCode})
        }

SMResponsePdu ::= CHOICE {
        resultPdu                       SMResultPdu {{ EFC-SM-Transactions}},
        errorPdu                        SMErrorPdu {{ EFC-SM-Transactions}}
        }

SMResultPdu {TRANSACTION: Transactions} ::= SEQUENCE {
        invokeId                        INTEGER,
        transactCode                    TRANSACTION.&transactionCode ({Transactions}),
        result                          TRANSACTION.&ResultType ({Transactions} {@transactCode})
        }

SMErrorPdu {TRANSACTION: Transactions} ::= SEQUENCE {
        invokeId                        INTEGER,
        transactCode                    TRANSACTION.&transactionCode ({Transactions}),
        error                           TRANSACTION.&ErrorCodes ({Transactions} {@transactCode})
        }
```

```
EFC-SM-Transactions TRANSACTION ::= { complianceCheck | summariseLog | monitorRecord }

-- Compliance check transaction

complianceCheck TRANSACTION ::= {
        ARGUMENT                ComplianceCheckArgument
        RESULT                  SignedSpotCheckData
        ERRORS                  {ComplianceCheckErrors}
        CODE                    3
        }

ComplianceCheckArgument ::= SEQUENCE {
        recordListIds           SEQUENCE OF ObjectId OPTIONAL,
        counterIds              SEQUENCE OF ObjectId OPTIONAL
        }

ComplianceCheckErrors INTEGER ::= {invalidArgument}

-- Summarisation transaction

summariseLog TRANSACTION ::= {
        ARGUMENT                SummariseLogArgument
        RESULT                  SignedSummary
        ERRORS                  {SummariseLogErrors}
        CODE                    4
        }

SummariseLogArgument ::= SEQUENCE {
        secureLogId             ObjectId,
        summarisationTime       DateTimeAndDiff
        }

SummariseLogErrors INTEGER ::= {invalidArgument}

-- Monitor Record transaction

monitorRecord TRANSACTION ::= {
        ARGUMENT                MonitorRecordArgument
        RESULT                  ObjectId
        ERRORS                  {MonitorRecordErrors}
        CODE                    5
        }

MonitorRecordArgument ::= SEQUENCE {
        secureLogId             ObjectId OPTIONAL,          -- absent for a new log
        record                  MonitoredRecord
        }

MonitorRecordErrors INTEGER ::= {invalidArgument}

-- SM transaction errors

otherError                      INTEGER ::= 0
serviceNotAvalible              INTEGER ::= 1
invalidArgument                 INTEGER ::= 2
invalidCertificate              INTEGER ::= 3
invalidSignature                INTEGER ::= 4
invalidReference                INTEGER ::= 5
invalidModuleTag                INTEGER ::= 6
invalidRequestdata              INTEGER ::= 7

END
```

C.7.2 The embedding of DRSC transaction into the ISO 15628 ASN.1 module

```
DSRCData { iso(1) standard(0) iso15628(15628) dsrcData (1) reducedVersion (17575) }
DEFINITIONS AUTOMATIC TAGS ::=BEGIN

-- Derived from ISO / DIS 15628
-- Everything not required to show how TS 17575 can make use of ISO 15628 is omitted.

IMPORTS
        SMRequestPdu, SMResponsePdu   FROM SecureMonitoringTransactionsModule;

Container::=CHOICE{
--      The values 1..71 are ommitted
        eriRequestPdu                   [72] SecureMonitoringTransactionsModule.SMRequestPdu,
                                        -- only to be used in an Action-Request
        eriResponsePdu                  [73] SecureMonitoringTransactionsModule.SMResponsePdu,
                                        -- only to be used in an Action-Response
        ... -- extension marker
        }

END
```