Secure monitoring and the use of trusted element counters

Jan Vis, July 29, 2010

Release note:
This paper is still a t draft that may contain contentious issue. In order to speed up the discussion a preliminary draft of those issues is included as well.

Contents

1 INTRODUCTION

1.1 Architecture

2 GENERIC COUNTER PROPERTIES

2.1 Guaranteed non-decreasing
2.2 TE: Counting or checking counting
2.3 The meaning of a counter
2.4 Leaving and re-entering toll domains
2.5 Auxiliary counter check information

3 SUPPORT OF THIN OBE

4 SUPPORT OF MULTIPLE TARIFF SCHEMES

4.1 Introduction
4.2 Tariff schemes to be supported simultaneously
4.3 Support of a distance based tariff scheme
4.4 Support of a length of stay based tariff scheme
4.5 Support of a passage based tariff schemes
4.6 Support when no fee is due

1 Introduction

This paper addresses some issues around the use of counters in OBE account records for secure monitoring.

References:

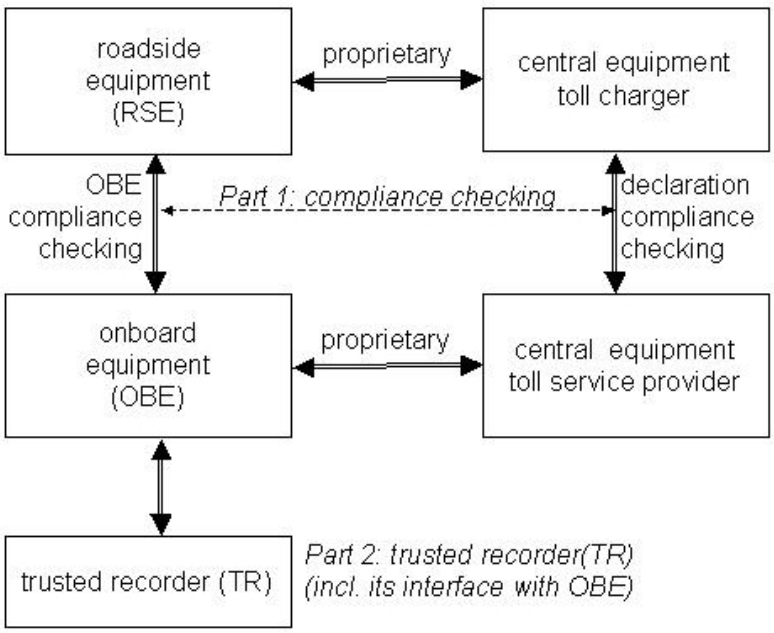
[1] An example of a view on EETS trust and privacy in GNSS based toll systems

1.1 Architecture

The Technical Specification on secure monitoring should specify the requirements for secure monitoring, a concept that allows checking the trustworthiness of the toll declarations from a toll service provider while respecting the privacy of the user of the vehicle.

Secure monitoring provides a toll charger with an autonomous toll system the tools to check whether or not an observed presence of a vehicle in his toll domain is correctly included in the account, i.e. in the set of records underlying a toll declaration.

The overall architecture is depicted in the figure below.



The trusted element is used by the OBE to make itself accountable to toll chargers. The trusted reorder has to be trusted by both the toll service provider and the toll chargers. The TE signs OBE account records with an adequate delay (see [1]).

An OBE account record is a record that summarises the onboard account at a certain time and location. On OBE account record contains at least a time / location stamp and the value of zero of more counters.

The time / location stamp contains the time and the location of the vehicle as perceived and recorded by the OBE.

When signed by the trusted element, the OBE account record is said to be frozen. The term 'element' is its name stems from the fact that it has to store the current value of the counters as well (see below).

The responsibility for keeping frozen OBE account records available for further processing rests on the toll service provider (and not on the toll charger). Consequently they can be stored in the OBE outside the TE.

2 Generic counter properties

2.1 Guaranteed non-decreasing

As shown in [1], counters shall be non-decreasing and this property shall be guaranteed by the trusted element.

2.2 TE: Counting or checking counting

The TE shall guarantee that counters are non-decreasing. This may be accomplished on one of the following ways:

1. The TE takes the counter values itself as input
   In this case OBE produces the OBE account records and, when freezing, the TE has to check that the counter values are not less than in the previous OBE account record.

   Note that this method requires also the use of flags (one per counter of one for all counters) to allow the TE to signal whether or not the counters are non-decreasing indeed.

2. The TE takes the increments as input
   In the case the TE is doing the counting and is producing and freezing the OBE account records.

   Note that in this case there is no need for additional flags. The TE can be made to interpreted the input always as positive value.

Note that, from a mathematical point of view, both methods are equivalent. Also, the same OBE account records are produced and in either case the TE has to retain the last counter values.

So the choice between these two method should be based on implementation costs and/or the need to keep the trusted element as simple / cheap as possible.

The major difference in this respect seems to be a minor one. In the first case the TE has to compare two values, to set a 'non-decreased' flag and to store the most recent value. In the second case the TE has to add an increment to the stored counter value and produce the OBE account record. With a clever design, this may accomplished by replacing the increment in its input with new counter value.

Although the differences are small, it is assumed that the second method may result in a slightly simpler TE.

Note that the issue addressed in section is relevant only for part 2. It has no consequences for the OBE compliance checking transaction specified in part 1.

2.3 The meaning of a counter

The use and meaning of a counter may vary from toll domain to toll domain and/or depend on the 'thickness' of the OBE. A counter may be used for a sequence number, a distance driven, an elapsed time, a number of passages, a fee due, etc.

The meaning the counters to be used in a OBE account record shall be 'known" by the OBE and the compliance checking RSE.

NOTE: For this paper it assumed that the toll charges assigns the meaning of the counters as part of his toll context data. And, in case he supports various types of OBE, this assignment may depend on the thickness of the OBE too.

However, in order to keep the design of the TE as simple as possible and, consequently, to make the TS a universal as possible, the TE should not be aware of the meaning of the counters in the various toll domain. In this case a new or changing toll regime may only affect the OBE and RSE but not the TE.

Note that by keeping the TE as simple as possible, it will be easier and cheaper to obtain a particular EAL (Evaluation Assurance Level) defined in ISO 15405 'Security techniques -- Evaluation criteria for IT security'.

2.4 Leaving and re-entering toll domains

Above, it is implicitly assumed that TE maintains the value of a counter when leaving a toll domain and continues the use of this counter when the vehicle re-enters this toll domain.

However, this approach should compares with the alternative that the OBE re-initialise the counters anytime the OBE re-enters a toll domain.

First, note that in either case the OBE should generate an OBE account record when the vehicle leaves or enters a toll domain and these records shall be frozen with the TE.

Maintaining the counter values per toll domain and even the one seldom visited would requires some memory. But this will not be excessive when compared with capabilities of a modern smart card.

A calculation example: 7 4-byte counters (incl. time) per toll domain with 4-byte auxiliary data and 8 bytes domain identification/description data would require 64 bytes per toll domain. So, circulation in 256 toll domains would require 16 kB. Assuming a maximum of at least 500 000 writes in a memory cell and knowing that there are 525 600 minutes in a most years, a 64 kB memory would result in a 4 year lifetime if every, every minute an OBE account record was frozen. But, with a clever per toll domain 'memory cell update' design this figure could be quite easily increased (with a maximum of 256 times).

Allowing counter resets would require additional measures to counter the associated risks. Without counter measures, OBE that has not been checked for a while might be reset the counters and after producing two correct OBE account records (the first one reflecting the distance to the border) the reset will not be noticed anymore. Of course one may think of a more complex reset operation with the use of some ‘reset counter’ that is not reset, but this

would impair the basis idea of the counter reset. (Note that there should be a ‘reset counter’ per toll domain).

So unless we can design effective and efficient counter measures, allowing counter resets would greatly reduce the value of spot-checking and would make the toll charger almost completely dependent on unobtrusive observations with checking the declaration afterwards.

2.5 Auxiliary counter check information

Compliance checking of a thick OBE may require also e.g. a vehicle tariff class in order to check whether the fee has been calculated correctly.

And, as a toll charger may use different vehicle classifications for different tariff schemes, the use of this class information might be ‘counter’ dependent.

One way to resolve this is to associate with each counter an auxiliary ‘class’ value with a meaning that is determined in the same way as the meaning of the counter.

NOTE: Static parameters could be included in a – possibly toll domain dependent - 'toll account certificate' TEC (see [1]). However, this is not possible for dynamic vehicle parameters like the number of axles.

3 Support of thin OBE

A thin OBE may only produce time/location records.

In this case, an OBE account record may not uses any counter, or may use one counter as a record sequence counter.

From a toll charger’s point of view there is little need for a sequence counter. The counter is not needed for checking a toll declaration afterwards and with spot-checking the OBE has to provide the compliance checking RSE only with the last two account records. Consequently, omitting a sequence number would open the door only for omitting the previous OBE account record and using an older one instead. However, this does not seem to be of any value for the toll service provider or for the user.

However, a toll service provider may use a sequence to detect some fraudulent behaviour of the user. Suppose that the user allows the OBE to create frozen OBE account records for on-spot compliance checking and then, e.g. if not being checked, deletes a number of records before their transmission to the toll chargers back-office. First note that the toll charger will detect this kind of fraud when the toll declaration is checked afterwards and the observed presence of the vehicle was deleted from the registered itinerary. However in this case the toll charger would be blamed. However, when using sequence numbers a toll charger can detect this kind of fraud and, e.g. blacklist the OBE or take any other measures.

NOTE 1: In either case, a ‘sequence number’ counter may be implemented as a standard counter. Non-increments can be checked by the RSE.

NOTE 2: Also, the use of sequence counter requires the transmission of all frozen OBE account records, i.e. including the signatures, to the back-office. For checking a declaration afterwards this is not required. Then, only the last one in a declaration period must be sent frozen.

This technical specification should support both options.

NOTE: It should be up to the toll charger to accept or not to accept this additional risk and to require or not to require the use of a counter for sequence numbering (see also the section above on the meaning of a counter)

4 Support of multiple tariff schemes

4.1 Introduction

This section applies only to OBE that is 'thick enough' to use tolled object and tariff scheme information.

4.2 Tariff schemes to be supported simultaneously

In order to be applicable in any toll domain, the following types of tariff schemes must be supported:

1. distance based tariff schemes,
2. length of stay based tariff schemes,
3. passage based tariff schemes.

And as one toll domain may deploy more than one tariff scheme, this technical specification should also support the simultaneous use of different (types of) tariff schemes. Consequently:

1. An OBE account record may need more than one counter
2. Different tariff schemes may require different moments to update the OBE account record.

4.3 Support of a distance based tariff scheme

Support of this tariff scheme is quite straight forward. The OBE will regularly produce a record indicating the toll due since the generation of the previous OBE account record. The TE will then add this increment to the total amount and produces and freezes a new OBE account record.

In toll due may be indicated directly by its value or, more indirectly by the distance driven under a specific fee for a unit of distance.

When supplied with the last to account records and the toll account certificate (TAC), the RSE can check the correctness over the itinerary between those last two records by subtracting the two counter values and checking whether or not the recorded fee corresponds with the distance travelled according to time / location stamps in these OBE account records and the vehicle tariff class information in the TAC.

For this type of tariff scheme there are no strict requirements for the update frequency of the OBE account record. However, incorrect behaviour may be hard to prove if the vehicle could not be observed during the whole itinerary reported in the last two OBE account records (if not a driver could make up any story for the period the vehicle could not be observed).

Note that 'not being observed' should require official report from officials. In most cases a simple video would suffice. For a motorway e.g., it would sufficient if such a video could show that there were no vehicles on the hard shoulder and that traffic was moving smoothly.

Also, when needed for another tariff scheme a regular period between two OBE account records may always be shortened because of the need for an account record for another tariff scheme.

4.4 Support of a length of stay based tariff scheme

For a length of stay based tariff scheme without a ceiling the same reasoning as for a distance based tariff scheme applies.

However, things may be a little bit different in case such a tariff schemes includes a ceiling, i.e. a tariff scheme with a maximum fee to be paid for a particular period. An example is a daily maximum as often used for parking.

With such a tariff scheme, the OBE may stop generating OBE account records for the rest of the period when the ceiling has been reached. However, the RSE used for compliance checking should be able to determine whether of not this has been really the case.

A easy way accomplish this trust is to create an OBE account record at the beginning of the period and to present this record to compliance checking RSE whenever the ceiling was reached.

In case the length of stay based tariff scheme is the only tariff scheme is use, OBE can provide the RSE with the following OBE account records:

1. The last two records as for a distance base scheme as long as the ceiling has not been reached
2. The OBE account record at the beginning of the period and the last OBE account record (which may be the one produced when the ceiling was reached).

In case the OBE has to deal with other tariff schemes as well, it has to provide the RSE with the following OBE account records:

1. Before the ceiling has been reached:
   The last two records as for a distance base scheme
2. After the ceiling has been reached
   The OBE account record at the beginning of the period and at least one OBE account record produced since the ceiling has been reached (which is sufficient for the tariff scheme at hand).

So in case the ceiling has been reached and the OBE has to deal with a distance based tariff scheme as well, the OBE has to present the RSE the OBE account record at the beginning of the period and the last two OBE account records produced because of the distance based tariff scheme.

4.5 Support of a passage based tariff schemes

In a passage tariff scheme, the toll due may depend on the passage only (like e.g. for using a stretch of a road, bridge, a tunnel, or a ferry) or on the last two passages (like in closed tolling networks).

In case the toll depends on one passage only, it will be sufficient if the OBE had produced one OBE account record before the passage and one while passing. However, the record before the passage shall be as short before that is not possible to use it for more than one passage.

In case the OBE has to deal with other tariff schemes as well, it has to provide the RSE with the following OBE account records:
1. the last OBE account record before the passage
2. any OBE account record after the passage

4.6 Support when no fee is due

There are no reasons to check the compliance of OBE when no fee is due. E.g. because of the time or day or because the vehicle is not passing a tolled object.

Therefore, the OBE shall not be required to present any OBE account records when no fee is due. However, in order be able the check the OBE account up to the boundary of any tolled object, the OBE may required to present these records within a limited distance and/or time as agreed between the toll charger and the toll service provider.

Whenever the toll domain or a a tolled object is entered or left, an OBE account record shall be generated and frozen.