TRUST and PRIVACY

in INTEROPERABLE AUTONOMOUS TOLLING

Jan Vis
Advisor, Ministry of Transport, Public Works and Water Management, Rijkswaterstaat
P.O. Box 5044, 2600 GA Delft, the Netherlands
+31 6 2451 4776, visjpmm@xs4all.nl

ABSTRACT

The widespread use of tolling requires provisions for users of vehicles roaming through many different toll domains. For autonomous toll systems one party (the toll service provider) provides the metering for the other parties, the toll domain's toll chargers. The toll service provider uses onboard equipment (OBE) installed in the vehicle to calculate the toll and draws up the toll declarations for toll chargers. In practice such a scheme will work only if the toll charger can check the trustworthiness of the declaration while on the other hand the privacy of the user should be respected as well.
The secure monitoring concept described in this paper provides this trust and privacy. OBE data can be checked on the spot and for toll declarations it can be checked whether the declaration account corresponds with unobtrusive observations of the vehicle in the toll domain. The concept is based on well known cryptographic techniques. For the OBE this requires the use of a trusted element (e.g. smart card) but does not impose any further security requirements on the onboard equipment. Therefore, secure monitoring may lead also to less expensive onboard equipment.

Disclaimer: Although the Dutch Ministry of Transport, Public Works and Water Management pursues secure monitoring for interoperable tolling, this is a scientific paper that does not represent or imply any official position of the ministry.

INTRODUCTION

THE NEED FOR TRUST AND PRIVACY

The widespread use of tolling requires provisions for users of vehicles that are roaming through many different toll domains. Users should be offered a single contract for circulating a vehicle in various toll domains as well as onboard equipment (OBE) that is interoperable

with the toll system in all these toll domains.

In Europe, for example, this need for interoperability has been officially recognised and legislation on interoperability has been adopted already. See Directive 2004/52 [1] and the subsequent decision of the Commission [2].

In autonomous toll systems no road side equipment is used to determine the toll due. OBE is used instead. Interoperability for these systems is based on third party metering. A toll service provider uses the OBE to calculate the toll for the various toll domains and sends the toll declarations to the toll chargers. Those toll declarations, i.e. statements that a vehicle was circulating within a toll domain, may be produced by the OBE or by the central equipment of the toll service provider.

In practice, such a scheme will work only if based on a security concept that provides a toll charger with the means to trust the declarations from a toll service provider without having to trust this provider itself (as was already emphasised in [3]). On the other hand such a security concept should provide also the means to protect the privacy of the user.

The secure monitoring concept described in this paper provides this trust and privacy.

SECURE MONITORING IN A NUTSHELL

Secure monitoring is a concept that provides a toll charger with effective means to ascertain the trustworthiness of a toll service provider's toll declarations while preserving the privacy of the user.

Secure monitoring enables a toll charger to check whether or not a (randomly) observed presence of a vehicle in his toll domain is correctly accounted for in the toll service provider's toll declaration. Secure monitoring uses well-known cryptographic techniques both to 'freeze' data in the sense that every change of this data afterwards can be incontestably detected and to produce incontestable results that will stand in court.

The secure monitoring concept includes two compliance checking transactions:

1. A real-time OBE compliance checking transaction to check the onboard account
   I.e. to check whether or not the presence of a vehicle has been correctly accounted for by the OBE.
   This transaction can be invoked by Roadside Equipment (RSE), including mobile or handheld enforcement equipment.
2. A toll declaration compliance checking transaction to check a declaration account
   I.e. to check whether or not the presence of a vehicle as (unobtrusively) observed by the

toll charger has been correctly accounted for in a toll declaration from the toll service provider.
This transaction can be invoked by the toll charger's central equipment and shall be performed by the toll service provider's central equipment.

In order to prevent fraud the first transaction requires an onboard (e.g. a smart card) trusted element (TE) to sign the OBE data.

Note that secure monitoring focuses on the data (the account) that underlies a toll declaration. Though it requires a TE for real-time checking of OBE data, the concept does not require a tamper proof OBE and, therefore, it may pave the way to less costly OBE.

HISTORY

This paper is based on a concept of secure monitoring that was already introduced for the Dutch 'Kilometerheffen' (kilometre charging) project in 2001. At that time the concept was triggered by a presentation by Wiebren de Jonge and has been further elaborated on since then in:

- internal notes within the Dutch Ministry of Transport and the Stockholm Group, see [9],
- the EU Expert group 12 report 'Security aspects of the EETS' [5]

Additionally, the concepts have been independently evaluated in Dutch universities resulting in the following papers:

- Privacy-friendly Electronic Traffic Pricing via Commits [6]
- Privacy protection and Different Payment for Mobility (in Dutch) [7]

This resulted in 2009 in the paper "An example of a view on EETS trust and privacy in GNSS based systems" [4]. For further details the reader is referred to [9].

OVERALL ARCHITECTURE

The overall architecture is depicted below. The architecture complies with the ISO standard IS 17573. The interface between OBE and RSE is used for OBE compliance checking and the interface between the toll charger's central equipment and the toll service provider's central equipment is used both for the exchange of toll declarations and for toll declaration compliance checking.

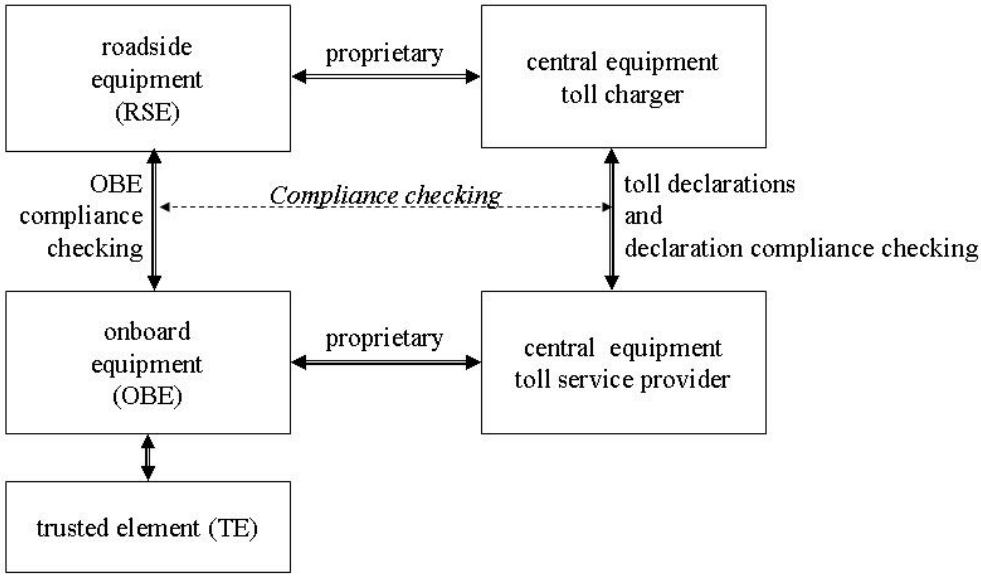

Figure 1. Overall architecture

TOLL DECLARATION COMPLIANCE CHECKING

BASIC IDEA

In GNSS (Global Navigation Satellite Systems) based toll systems, a toll charger should be able to judge the correctness and trustworthiness of the toll declarations from a toll service provider.

In secure monitoring this judgement is based on the following:

1. a toll charger may observe the circulation of vehicles in his toll domain unobtrusively, randomly and unexpectedly.
2. a toll charger can check whether or not the account that underlies the toll declaration indicates the presence of an observed vehicle at that time and location.
3. a toll charger can check whether or not the accounted presence of a vehicle is correctly included (in the total fee) in the declaration as received from the toll service provider.

Note that a toll charger can only trust these checks if:

1. The toll service provider cannot anticipate a check
   This requires that the vehicle is observed unobtrusively. If not, the toll service provider could draw up a correct account when checked and an incorrect one when not.
2. Nobody can modify the account unnoticeable when it is checked
   If not, one could always produce the desired response.

In secure monitoring this trust is based on the use of an incontestably 'frozen' declaration account. An account is said to be frozen if any change afterwards can be incontestably detected (e.g. by the toll charger).

At a first glance, an account can be frozen easily and incontestably by signing it completely and by sending the signature together with the declaration to the toll charger. Privacy seem to be guaranteed and a toll charger needs to receives only a declaration with a total amount. The correctness can be verified afterwards because the signature has frozen the account.

However, a problem arises when a toll charger wants to check only one single record in the account. By using just one signature over the complete account, the toll service provider has to provide him with the complete account in order to allow him to check the signature. This would unnecessarily violate the privacy of the user.

MULTI LEVEL FREEZING OF A DECLARATION ACCOUNT

Introduction and overview

Multi-level freezing provides the same trust to a toll charger as the coarse method with one single signature for the complete declaration account while, at the same time, protecting the privacy of the user.

The basic idea of multiple level freezing stems from [1]. It allows one to design security measures with a trade off between confidentiality and efficiency in terms of processing, storing and communication cost.

In the following sections first, the so-called hash-function is introduced. Then, the concept of multi-level freezing is presented with a simple example and shown to be able to provide the toll charger with the same level of trust and the user with a much higher degree of privacy. Next, some variants, details, and trade offs are discussed that may be used to improve the implementation of the concept.

Hash functions

A hash function is a function that maps strings of bits to fixed-length strings of bits called hash codes, satisfying the following two properties (see [8]) :

1. for a given hash-code, it is computationally infeasible to find a string of bits which maps to this hash-code; and
2. for a given input, it is computationally infeasible to find a second input which maps to the same hash-code.

So, by calculating and providing the hash code of an account (or a record), it is always possible to check whether that account (or record) has been changed. This is done by recalculating the hash-code and checking whether it has still the same value or not.

Note that a (digital) signature is also a hash-code with the additional property that its calculation can incontrovertibly attributed to an entity. Namely the one who possesses the private key needed for the calculation.

Two definitions

A record in a frozen account is called a frozen record if the hash-code for that record is included also in that frozen account.

The term multi-level freezing is used when not only the complete declaration account is frozen, but also individual records, i.e. if the hash-codes for individually frozen records are frozen too (see the example below).

An example of multi-level freezing for monthly declarations

As an example, and as depicted in the figure below, suppose the account for a monthly declaration contains the following records:

1. frozen hourly records with the itinerary of the vehicle during one hour;
2. a frozen monthly summary record with for each hour a fee is due a sub-record with the hourly fee and the hash code of the corresponding hourly record. Optionally, the total monthly fee may be included as well.

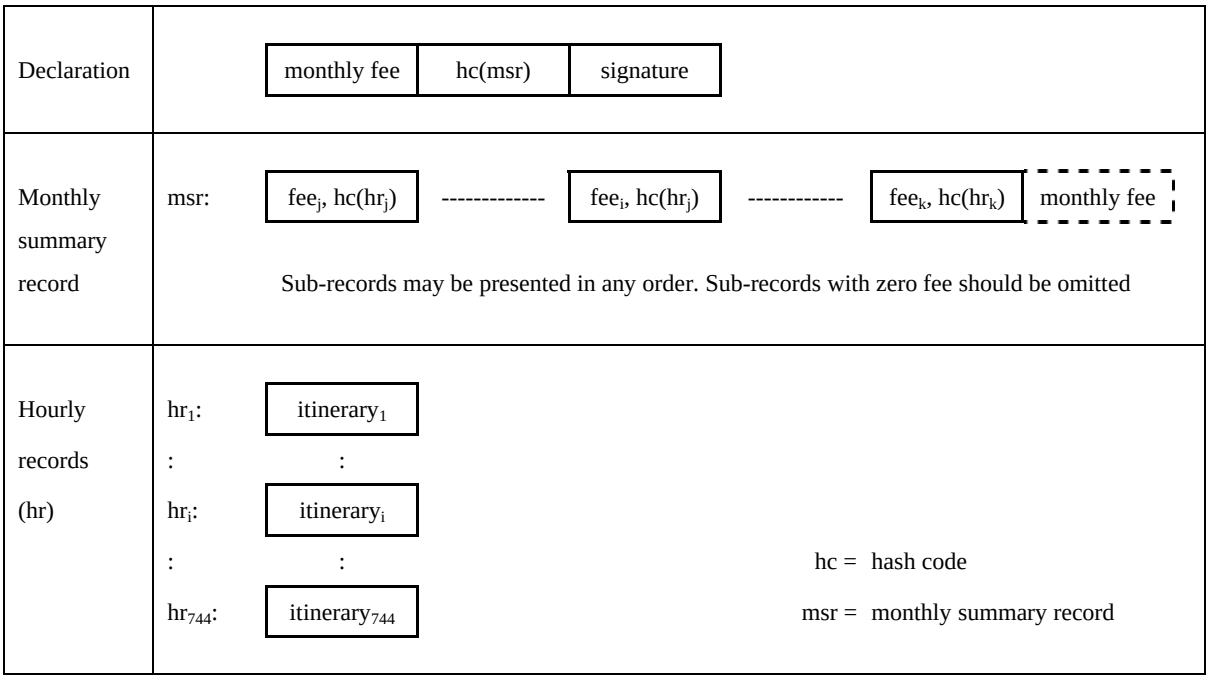

Figure 2. An example of multilevel freezing

The signed monthly declaration that is sent thus to the toll charger needs to contain only the total fee and the hash-code for the monthly summary record.

When the toll charger has received this signed declaration, he can ask for each observation of the vehicle the hourly record and the monthly summary record. Then, he can check whether or not:

- the observed presence of the vehicle was accounted for,
  (the itinerary in the hourly record should be in accordance with his observation),
- the hourly fee was correctly calculated and included in the monthly summary record,
  (the monthly summary record has to contain a sub-record with the hash-code of the hourly record and the correct fee)
- the monthly fee as reported in the declaration has been correctly calculated from the hourly fees.
- The hash-code for the monthly summary record equals the hash-code received with the toll declaration.

If all these check are positive he can trust the observed presence of the vehicle was correctly accounted for in the toll declaration received.

The privacy of the user is respected also. The toll service provider only revealed the hourly itinerary record for a location where the vehicle was already observed. And, for the other fee in the monthly summary record it was not even revealed for which hour that fee was due (the sub-record associated with revealed hourly record is by identified by its hash-code).

Note that in case there is no fee due for a particular hour, there is no need to include a sub-record with a zero fee in the monthly summary record. After all, there is no need to proof that a zero fee was correctly included in the total fee.

VARIATIONS, DETAILS AND TRADE-OFFS

Granularity and using more than one level

The amount of data needed to check an observation can be further reduced by using more levels: e.g. itinerary records per minute, hourly summary records, daily summary records, weekly summary records and monthly summary records.

There is also a question about the granularity of the account, i.e. how fine or coarse the basic itinerary description should be. In general, the distance between two points in time / location should not be longer than the period in which the vehicle could be observed. After all, one

may not be able to prove any non-compliance when the vehicle could not be observed.

No risk of extra fraudulent records

At a first glance the method may be vulnerable for the inclusion of extra fraudulent sub-record in the summary records. However, as a summarised value depends on the sum of non-negative sub-record values, such adding would only add to the declared toll and is of no concern for the toll charger.

Variants for different type of tariff schemes

Note this method can be used for all kind of tariff schemes. A fee per kilometre driven, a fee per unit of time (e.g. with or without a daily maximum), and a fee per passage are all supported. For details see the paper on counters via [9].

Accuracy issues

Even accuracy issues can be coped with. As a calculation of the toll for a recorded itinerary can be easily checked, inaccuracy may be only a problem if the recorded itinerary differs from the actual one. For a toll charger this may have negative consequences in case of recording a short cut or recording the use of a cheaper parallel road. Both can be dealt with by choosing points of observation which reveal those inaccuracies.

Processing and storage locations: OBE or central equipment

Note that it is immaterial for the trustworthiness of a declaration where the account records are processed or where they are frozen. This may be at the OBE, the toll service provider's central equipment or a combination of both.

With respect to the privacy, implementations where the OBE does not have to reveal location data to the central equipment of the toll service provider are, of course, to be preferred.

Summary of declaration compliance checking

Multi-level freezing of a declaration account can be accomplished with proven technology (hash-codes) and provides a means for a toll charger to check the correctness of a declaration based on his (unobtrusive) observations. The method is secure and can be implemented in a privacy-friendly way.

REAL-TIME OBE COMPLIANCE CHECKING

Introduction

For declaration compliance checking the freezing period coincides with a declaration period

and, as noted, a toll charger has to wait with its checks until he has received the signed declaration with the hash-code. Also, the observation of the vehicle should be unobtrusive.

However, this declaration compliance checking has serious and fundamental disadvantages:

1. With video surveillance it cannot be determined whether or not the vehicle is equipped with an accepted OBE and who the toll service provider is .
2. If the compliance of the account cannot be checked on the spot a vehicle may have left the country before any violation can be noticed.

Real-time freezing, allowing for on-the-spot compliance checking, can remedy this problem.

Real-time compliance checking

With real-time compliance checking an account is frozen each time a new record is added to this account. The last record(s) can then be used to check whether or not the observed presence of a vehicle was correctly recorded in the onboard account. Such a check can be performed on the spot without stopping the vehicle from the roadside. This can be done from the roadside, from another vehicle ,or with handheld equipment using DSRC or infrared.

An onboard account record suitable for real-time compliance checking shall contain then the following data:

- a time / location stamp
- the accumulated or incremental (see below) values of counters, e.g. counters the distance driven, the time spend or the fee due in/for a toll domain.

In addition, and see below details, the data to be provide to the compliance checking equipment should contain also a trusted element certificate and a toll account certificate.

With real-time OBE compliance checking, a toll charger should have confidence that the following conditions are met.

1. The account was frozen before OBE could notice a checking attempt.
2. The last record links up correctly to the previous one.
3. The account does not contain extra and therefore fraudulent records.
4. The declaration is based also on the checked account.
5. The declaration is correct also for the last part of the declaration period, i.e. for the part after the last on-the-spot check in that period.
6. The toll service provider responsible for the OBE can be identified.

If these conditions are met, a toll charger can trust an OBE account as much as a declaration account with declaration account checking.

Trust that the account was frozen when checked

When a vehicle is interrogated it is necessary to prevent the possibility that the onboard account can be quickly 'fixed' when the OBE notices a possible check (e.g. the presence of a DSRC beacon) and before the OBE responds on a check.

However, this kind of fraud can be prevented if one can guarantee that the time to freeze the onboard account for a new record is significant longer than the (short) time available for a compliance checking (DSRC) transaction.

A solution is to use a trusted element (TE), i.e. a device that is trusted by both the toll service provider and all the toll chargers and that can sign the account record with a adequate delay.

A TE may be implement e.g. as a smart card with a dedicated trusted function for signing data with a delay. The card should be issued then by a trusted third party together with a certificate to guarantees that the public key verifies the signature of a TE.

Trust that the last record links up correctly to the previous one

This can be most easily resolved by including the last two records in a compliance checking transaction.

As records should contain a time and location stamp as well as the accumulated or incremental value of the counters used, there can be no gap and the correctness for the interval between these record can easily checked. In case accumulated values are used, their difference shall correctly reflect the itinerary as indicted by the locations stamps and at the time indicated by the time stamp. In case incremental values are used, the values in the last record can checked in the same way. Note that in the latter case the accumulated values must be stored on the TE and that the TE has to add the increments to the accumulated values when signing the record with an adequate delay.

Trust that the account does not contain extra fraudulent records

As with real-time checking only the last two records are checked. Any 'older' record will not be noticed anymore. However this problem can be easily remedied as well. First note that a toll charger would not care any extra increments of a counter (e.g. for the distance drive or the toll due). So only decrements are to be precluded.

One way to solve this, is to store the accumulated values on a TE that can accept only positive increments. Alternatively, in case the onboard account is based on accumulated counter values, the TE should sign a record only if no counter value has been decreased.

Trust that the declaration is based also on the checked account

The toll charger should be sure that the OBE cannot use two accounts: one to be checked and one for declarations.

This can be accomplished by requiring that accumulated counter values in the onboard account are signed at the end of the declaration period by the TE and added to declaration. Then, it can be checked that the same signature (and hence the same TE) is used and that complete OBE account has been used for this declaration.

Trust that the declaration is also correct after the last check

At a first sight, the last part of a declaration period, i.e. after the last real-time check in that period might look vulnerable for fraud.

However, as the same methods can be used to assure that is no gap between subsequent declaration periods as can be used to assure that there are no gaps between subsequent records (see above), this is not a real treat. As long as a real-time check cannot be predicted, one can close a declaration period and continue with a subsequent period at any time.

Trust that the toll service provider can be identified

In order to allow the toll charger to identify the toll charger responsible for declaring the toll for a vehicle, the data returned to the compliance checking equipment should also contain a toll account certificate. I.e. a certificate in witch a toll service provider guarantees that he uses a particular TE for a vehicle with a particular registration number.

Note that this toll account certificate shall be well distinguished from the TE certificate. They serve a different purpose and have different parties responsible for their contents also.

Summary of OBE compliance checking

Real-time compliance checking provides a toll charger with the means to check the correctness of an onboard account with a trusted element and proven technology. The method is secure and can be implemented in a privacy-friendly way.

REFERENCES

[1] EU Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community (OJ L 166, 30.4.2004)

[2] C(2009) 7547, COMMISSION DECISION of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements (OJ L 268/11 13.10.2009)

[3] The Role of Financial Institutions, Payment and contractual aspects of EETS, 17 October 2006, Prepared by Expert Group 7 Working to support the European Commission DG TREN in the work on Directive 2004/52/EC. http://its-europe.org/download/rci_public_documents/Expert_Groups/EG_7_rapport_final_17_octobre_2006.pdf

[4] An example of a view on EETS trust and privacy in GNSS based systems, 15-12-2009 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/12/15/an-example-of-a-view-on-eets-trust-and-privacy-in-gnss-based-toll-systems.html

[5] Security aspects of the EETS , April 5th 2007, Prepared by Expert Group 12 Working to support the European Commission on the work on Directive 2004/52/EC. http://www.ertico.com/download/rci_public_documents/EG_12_Final_Report_v1.0_5apr07.pdf

[6] Wiebren de Jong and Bart Jacobs, Privacy-friendly Electronic Traffic Pricing via Commits, to be published in LNCS (Lecture Notes in Computer Science) by Springer. (also available via http://www.tipsystems.nl/)

[7] Prof. dr. E.R. Verheul c.a., Radboud Universiteit Nijmegen, RDW Privacybescherming Anders Betalen voor Mobiliteit (Radboud University Nijmegen, RDW Privacy protection and Different Payment for Mobility, in Dutch), version 1.0, April 2, 2008. http://www.cs.ru.nl/E.Verheul/papers/DS/ABVM.pdf or via http://www.cs.ru.nl/E.Verheul/papers/outline.htm

[8] ISO/IEC 10118-1:2000, Information technology — Security techniques — Hash-functions — Part 1: General

[9] For further papers on details and the historical background see: http://www.xs4all.nl/~visjpmm/papers/Secure%20monitoring/summary.html