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

Jan Vis,
Ministry of Transport, Public Works and Water Management
the Netherlands, March 12th, 2009

Foreword

The aim of the EETS, the European Electronic Toll Service, is to allow the user of a vehicle to conclude one service contract and to use one OBE for driving through all electronic toll domains in Europe.

Within the EETS a toll charger has to accept vehicles with onboard equipment (OBE) from a third party, the EETS provider, and to utilise toll declarations received from this EETS provider.

This paper deals with measures that can provide on the one hand a toll charger with a sufficient level of trust in the correctness of the toll declarations from an EETS provider while on the other hand protecting the privacy of the user.

This paper has been written to support the 'secure monitoring' as pursued by the Dutch of Transport, Public Works and Water Management for the EETS.

This paper aims to bridge the gap between the layman and the professional. By focussing on the high-level, conceptual issues it should be comprehensible for the layman with only a common knowledge of the EETS and security. Technical details that may be of interest to experts are provided in footnotes.

This paper is written in a top down fashion. Starting from the high level requirements for trust (by the toll charger) and privacy (for the user), it elaborates / refines solutions based on techniques that are nowadays commonly used. As a consequence the reader is urged to be a little bit patient. When dealing with an issue, the basic concept is presented before its applicability and before elaborating on the drawbacks and optimisations. Consequently, a reader may skip at a first reading the more detailed remaining sections on the same level.

Disclaimer
Although the Dutch Ministry of Transport, Public Works and Water Management pursues secure monitoring for the EETS, this paper is a technical paper and does not present or imply any official position of the ministry.

Contents

1. Introduction

1.1 EETS, GNSS based toll systems and security

The European Electronic Toll Service (EETS) is a service which allows a user to conclude one contract with an EETS provider and have his vehicle equipped with one OBE in order to use this vehicle in all toll domains in Europe that require OBE.

In GNSS based toll systems an EETS provider sends the toll charger toll declarations, i.e. statements that a vehicle was circulating within a toll domain. Those declarations may be submitted directly by the OBE or by the central equipment of the EETS provider based on data obtained form the OBE.

In practice, such a scheme will only work if the toll charger can trust the declarations from an EETS provider without having to trust the EETS provider[1]. One way to provide this trust is secure monitoring[2].

However a major consideration is that privacy legislation requires that no more information be passed to a toll charger than necessary for his business. i.e. collecting a correct toll. At the same time a user may require detailed data to check the invoice and/or to pass on the fee for particular trip to his customers[3,4].

As shown below, secure monitoring can provide both an adequate level of trust and of confidentiality. The major design trade-offs are not between trust and confidentiality, but between trust and confidentiality on one hand and the operational processing, storage and communications cost on the other.

1.2 History

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

- internal notes within the Dutch Ministry of Transport and the Stockholm Group [10],
- the EU Expert group 12 report 'Security aspects of the EETS' [3]
- Annex C of an old draft of ISO TS 17575 [4],

In addition, the concepts have been independently evaluated in Dutch universities which resulted in the following papers:

- Privacy-friendly Electronic Traffic Pricing via Commits [1]
- Privacy protection and Different Payment for Mobility (in Dutch) [5]

The terms 'secure monitoring' and 'trusted element' stem from the EU Expert group 12 report “Security aspects of the EETS” [3].

The use of the term 'freeze' and its derivates stem from the paper of Wiebren de Jonge and Bart Jacobs [1].

[1] The basic fact that the EETS should not be based on the premises that an EETS provider and a toll charger should trust each other is also stressed in Comité Télépéage and Expert Group 7 report 'The Role of Financial Institutions' [2].
[2] Secure monitoring starts with the protection of the data, not with the protection of OBE (e.g. by making the OBE tamper-proof)
[3] In particular, this may be the case for haulers, taxi drivers, or car rental companies.
[4] However, as this requirement has no consequences for interoperability, it is not dealt with in this paper.

2. Secure monitoring

2.1 The basic idea

In GNSS based toll systems, a toll charger should be able to judge the correctness and trustworthiness of the toll declarations from an EETS provider.

In secure monitoring this judgement is based on the following:

1. the toll charger may observe the circulation of vehicles in his toll domain[5].
2. a toll charger can check whether or not the EETS provider's account 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[6] as received from the EETS Provider.

Note that a toll charger can only trust these checks if nobody can modify the account for a declaration. Otherwise one could use a correct account when noticing that the toll charger has observed the presence of the vehicle and an incorrect one when not.

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[7] the complete account and to send the signature together with the declaration to the toll charger: privacy is guaranteed, 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 EETS 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.

Moreover, the toll charger has to wait to perform his inspection until the account is frozen, i.e. until he receives the signature.

As shown below, both problems can be remedied:

- First, the need to provide a toll charger with a complete account can be avoided easily by using multi-level freezing.
- Second, the freezing of the account for a declaration may be augmented with a real-time freezing of the onboard accounts with a trusted element. This allows then for an on-the-spot checking of these on board accounts.

[5] At this point it is immaterial how this presence is observed. Differences between DSRC and video surveillance are addressed in section 2.3
[6] I.e. whether a correct fee is used for an observed part of the vehicle's itinerary and whether that fee is correctly included in a declaration.
[7] Questions about the key used for signing and the responsibility for the signature are deferred to section 3.

2.2 Multi level freezing of a declaration account

2.2.1 Introduction and overview

In this section a privacy friendly multi-level freezing of accounts is elaborated which provides the same trust to a toll charger as the coarse method with one single signature for the complete declaration account.

The basic idea of multiple level freezing stems from [1]. In essence, 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 in a simple example and it is shown that it can provide both 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.

2.2.2 Hash functions

A hash function is a function which maps strings of bits to fixed-length strings of bits called hash codes, satisfying the following two properties (see [6])[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 calculation the hash of an account (or a record), one can always check whether the account (or record) has been changed 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).

2.2.3 Two definitions

A record in a frozen account with a hash-code over that record is called a frozen record.

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).

2.2.4 A simple example of multi-level freezing for monthly declarations

As an example[9], suppose the account for a monthly declaration contains the following records:

1. frozen one-hour records with the itinerary of the vehicle during one hour and the fee due for that hour[10]

[8] The computational feasibility depends on the specific security requirements and environment. The most well known hash function is sha1 (see [7] and [8]). In the mean time sha1 has been succeeded by sha2 (see [8] and http://en.wikipedia.org/wiki/SHA_hash_functions for an overview.

[9] This example is constructed to explain the idea, for optimisations see the section below.

[10] So the one-hour record hr_i for hour i contains both the itinerary i_i and fee f_i for that hour. And as the record is frozen also $h(hr_i)$, the hash-code over hr_i is calculated.

2. A frozen monthly summary record with hourly fees due and the total monthly fee (being the sum of the hourly fees)[11].
3. A frozen monthly hash-code record with the hash-codes of the hourly records and the hash-code of the monthly summary record[12,13].

Then, the signed monthly declaration to be send to the toll charger needs to contain only:

- the total fee and
- the hash-code for the monthly hash-code record to freeze the complete declaration account

When the toll charger has received this signed declaration, he can:

1. ask, for each observation of the vehicle, the hourly record with the itinerary for that hour and then check whether or not:
    - the observed presence of the vehicle has been accounted for (the recorded itinerary should be in accordance with his observation)
    - the hourly fee has been correctly calculated for the recorded itinerary
2. ask for the monthly summary and check whether or not:
    - the hourly fee was correctly included in the record
    - the monthly fee has been correctly calculated from the hourly fees.
3. ask for the monthly hash-code record and check whether or not:
    - the hourly record he has received is indeed part of the frozen account (by checking whether or not this record contains the hash-code of the hourly record)
    - the monthly summary record he has received is indeed part of the frozen account (in the same way as for the hourly record)

Other examples can be found in [1].

Firstly, note that in the example above, for each observation of a vehicle only access is needed to one hourly record and the monthly summary record . This is considerably less then for the account with only one hash-code over all records (in which case the toll charger would need the complete account in order to check the hash-code).

Secondly, note that the toll charger has received all the information needed to check whether the observed presence of the vehicle was correctly accounted for, or not. It can also be verified that the part of the declaration account he did not receive was not needed for this check.

Thirdly, when asking for an hourly record the toll charger may be asked to provide his observation details (time location) as well. And, the EETS provider may be allowed to provide the requested data only if the claimed observed presence is reflected in his account. If there is a conflict, there is no immediate need to show the different record(s) to the toll charger and it will depend on the subsequent procedure to whom he might have to reveal this data.

[11] So the monthly summary record msr contains the monthly fee mf and the one-hour fees f_1, …, f_n, where n equals the total numbers of hours in the month. And as the record is frozen,, also h(msr), the hash-code over msr is calculated.
[12] So the monthly hash-code record mhr contains the hash-code h(msr) for the monthly summary record, and the hash-codes h(hr_1), …, h(hr_n) of the one-hour records (see note 10). And, as the record is frozen, also h(mhr), the hash-code over mhr, is calculated.
[13] Note the correspondence between msr, the monthly summary record, and mhr, the monthly hash-code record. In essence, the mhr freezes the calculation the msr.

2.2.5 Variations, details and trade-offs

2.2.5.1 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 record per minute, hourly summary records, daily summary records, weekly summary record and monthly summary record. The maximum confidentiality is achieved when every summary record summarises only two subordinate records.

Note that, for each intermediate result, the calculation for that result shall be frozen as well[14]. Basically, each accounting structure shall be mirrored in a corresponding hash-code structure in accordance to generic rules that can be implemented with well-known algorithms.

In general one has to make a trade-off between acceptable level of confidentiality (privacy protection) and the operational cost for data processing, storage and communication[15].

2.2.5.2 The granularity of the account

The example above was based on hourly records. To make them useful, they should contain the vehicle's complete itinerary for that hour. This raises the question of the granularity of the account, i.e. how fine or coarse should the itinerary be[16].

Generally speaking, with an account with finer granularity in the base records, less data needs to be revealed but the account will be larger than one with coarser granularity in the base records.

In case the account would contain all GNSS location fixes as base records, an observation at some point in time would only reveal the itinerary from one GNSS fix to the next one that contains the time of the observation. This works but would require a huge accounting effort.

Although the subject requires further study, 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 non-compliance if the vehicle's user if free to make up a story for any period that the vehicle could not be observed[17].

2.2.5.3 Including the hash record in the summary records – a more privacy friendly alternative

In the example above there was a separate record to summarise the fee (the monthly summary record) and a record to summarise the hash-codes. For both records it was assumed that the hourly (hash-code) data was indexed by the hour-number within the month

Alternatively, both records can combined in one record with hourly sub-records that contains both the hourly fee and the hash-code over the hourly record[18].

---

[14] I.e. each intermediate result shall be recorded in a frozen intermediate result record irr that contains the intermediate result value irv as well as the values v_1 to v_n from subordinate records sr_1,.., sr_n used to calculate this ivr. And, in addition, a frozen intermediate hash-code record ihr with the hash-codes h(irr), h(sr_1), …, h(sr_n) for respectively irr, sr_1, …, sr_n shall be recorded as well. See also footnotes 11-13.

[15] E.g., four values a, b, c, and d may add at once as (a+b+c+d), in two levels as e.g. ((a+b)+(c+d)), or in three levels as e.g. (((a+b)+c)+d) as long as the calculation method is fixed in advance and. does not depend on the value to be checked.

[16] I.e. the granularity of a multi-point itinerary in some record or the granularity of atomic records with only one point (for which the itinerary has to be constructed from sequence of records).

[17] E.g. I was waiting for half an hour around the corner or I made a stop for an hour on the hard shoulder.

[18] So the monthly summary record msr contains then the monthly fee mf and the sub-records (f_1 ,h(hr_1,), …, (f_n ,h(hr_n,) with the one-hour fees f_1, …, f_n, and the hash-codes h(hr_1), …, h(hr_n) over the one-hour records and where n equals the total numbers of hours in the month. As the record is frozen, also h(msr), the hash-code over msr is calculated.

Note that in this alternative, an hourly fee in the summary record can be identified by the hash-code over hourly record and that in this case the sub-records may be presented in any order[19,20]. If e.g. ordered with increasing hash-code values, a toll charger can determine the fee related to particular hour, but for the other hourly fees it is not revealed for which hour this fee was due.

2.2.5.4 A few examples

Suppose that one wants to combine at some intermediate level daily records into one weekly record. This can be accomplished in several ways, one might:

1. add all the daily records at once to one weekly record (Mo+Tu+We+Th+Fr+Sa+Su)
2. introduce an intermediate level, e.g. ((Mo+Tu+We)+(Th+Fr)+(Sa+Su))
3. or combine each day with all the previous days: ((((((Mo+Tu)+We)+Th)+Fr)+Sa)+Su)
4. include only those days for which a fee is due

Note the first example is the most efficient but any check for some observation within some week will reveal also all other daily totals. The second example is computationally somewhat more complex – one has to cope with an additional level and additional hash codes –, but will reveal less information for a check.

At a first glance, the third example looks computationally attractive. One only has to add each new daily total to the total of the previous days. However when checked, it depends on the day to be checked. In case an observation on a Sunday is checked, one only has to reveal the data for the Sunday and the total for Monday till Saturday to show that the fee due for Sunday has to properly included in the weekly fee[21]. However in case an observation on Monday has to be checked, one has to reveal all the other daily totals to allow the toll charger to check all the additions.

In the first three examples every day has its fixed place in the weekly addition. If we should want to skip the days for which no fee is due this cannot be the case. In that case (example 4) the weekly sum is made up from non-zero daily fees identified by their hash-code. If the toll charger should want check the observed usage of a vehicle, one has to reveal the data for that day and the inclusion of that day in the weekly addition is then identified by the hash-code of the daily record[22,23].

The fourth example also accommodates vehicles circulating outside the toll domain. After all, there is no need for a toll charger to know the vehicle's itinerary outside his toll domain. This example may be implemented by means of the alternative presented in the previous section 2.2.5.3.

---

[19] Due to their almost uniqueness of hash-codes (it is not feasible to find a second record with the same hash code),the inclusion of the right combination of .the hash-code and fee from the hourly record in the summary record will provide an almost certain proof that hourly fee was included in the summary record. The change of duplicates is one out of many, many billions.

[20] Using mathematical formulas, in the original example the monthly fee was calculated from the hourly fees using an index over the hours, i.e. $\sum_{i=1}^{max} f_i$ where f_i is the fee for hour i in the month. In the alternative the total fee was calculated as $\sum_{h \in H} f_h$ where f_h is the fee for the hourly record identified by hash-code h in the set of all hourly hash-codes H.

[21] This variant will be used for real-time freezing (with some additional measures), see 2.3.

[22] So, even if the daily fee for two days should be exactly the same, the value for a particular day can be determined using the hash-code for the daily record. See also the alternative described in 2.2.5.3.

[23] And, if one should want to check an observation of the vehicle when it was not use, the answer will simple be "no data available, so no fee due in relation to this observation". Indeed, such a check is useless.

2.2.5.5 No risk for extra fraudulent records

In the example it could be checked easily that the declaration was not based on extra fraudulent records that would never appear in a check. For each month the number of hours can be calculated and checked in the monthly summary record.

However, even if the number of subordinate records in a summary record is not known[24], there is little risk of any additional fraudulent subordinate record. A declared fee is the sum of the non-negative fees for smaller (time) units and this can be checked.

So an additional fraudulent subordinate record would only be unnoticed in case it would add to the fee (and would be robbing the user's own purse).

2.2.5.6 Using only one request from the toll charger

The three requests from the toll charger above can be reduced to only one. Generally speaking, when a toll charger presents the time/location details of an observation of a vehicle to the EETS provider, the EETS provider shall provide him with the record(s) that accounts for the presence of a vehicle at a certain time and location and the records proving that the fee due in relation to the location record(s) is correctly included in the declaration[25].

2.2.5.7 Variants for different type of tariff schemes

In the example above the declaration was based on hourly records. However for a particular toll domain other solutions may be preferred. E.g.:

1. for a fee per kilometre driven, there may be a record for e.g. every km driven in a tolled object and/or for a particular fee.
2. for a fee per unit of time, there may be a record for every minute of presence in a tolled object and/or for a particular fee.
3. for a fee per passage, there may be a record for each passage.

Note that in case there is e.g. a record per km, the EETS provider should still be able to reveal the right km-record if a toll charger has observed the usage of a vehicle. Showing that the km-fee has been correctly incorporated in a declaration can be done in a same way as in the previous examples above.

2.2.5.8 Other declaration variants

Depending in the contractual relation between the EETS provider and the toll charger an EETS provider might be required not to declare the total fee, but one or more basic values like the distance driven for some fee level (i.e. for a fee per km), the time spent for some fee level (i.e. for a fee per unit of time), or the number of passages (for a fee per passage).

This might be required for different reasons. First it avoids the necessity to inform the EETS provider and, if applicable, the OBE of the actual fee levels. Second, the toll charger might need a more itemised declaration in case the fee resulting from different tariff schemes is questioned.

However, this may result in a more complex declaration but does not influence the possibilities to freeze a declaration account.

[24] See the fourth example in 2.2.5.4 above.
[25] Note that the toll charger shall know the syntax and the semantic of these records, i.e. the accounting rules, as well.

2.2.5.9 Differences one might have to deal with

Due to differences in signal processing, there might be always some difference between a location[26] in the account and the location as observed by the toll charger. Eventually, this difference can be used for a KPI (key performance indicator) for the accuracy of the OBE.

2.2.5.10 Processing and storage locations: OBE or central equipment

Note that with regard to the trust, it is immaterial where the account records reside, where they are processed or where the account is frozen. This may be the OBE, the EETS provider's central equipment or a combination of both. What counts for the trust, is that the complete account for a declaration is frozen and that a toll charger knows where he can ask for the required data.

Nevertheless a toll charger should know where he could ask for his inspections: should he have to address the OBE or the central equipment of the EETS provider. In case all the processing is performed in the OBE, the OBE might be the most obvious. In case the declaration was processed with the central equipment, the central equipment would be the obvious address.

Note that in either case, regular inspections can be fully automated. In case the toll charger provides the EETS provider with the time / location details of his observation of the vehicle, all the data to prove the correctness of the account with respect to this observations can be automatically retrieved from the frozen account (see 2.2.4)

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

2.2.6 Summary of multi-level freezing

Multi-level freezing of a declaration account can be accomplished with proven technology (hash-codes) and provides a means for a toll charger the check the correctness of a declaration based on his (unobtrusive) observations.

The method is secure and can be implemented in a privacy-friendly way. However a toll charger cannot do his inspection of the account until he has received a signed declaration with the freezing hash-code.

To conclude, the multi-level frozen declaration account of a EETS provider can be securely monitored when the declaration has been received by the toll charger.

2.3 Real time freezing

2.3.1 Introduction

In the examples above, the account for a declaration was frozen when the (monthly) declaration was send to the toll charger. This freezing where a freezing period coincides with a declaration period, is called freezing per declaration.

As noted, a toll charger has to wait to perform his inspection until the account is frozen, i.e. until he receives the signed hash-code. Because, if a vehicle’s observation should become known before the account is frozen the account may be corrected. Consequently the toll

[26] Time can be measured accurately (and in include in the GSS signal that can used by both the OBE and observing equipment).

charger should not use DSRC (Dedicated Short Range Communication) but, e.g., unobtrusive video surveillance with automatic licence plate recognition[27].

However, freezing per declaration has serious and fundamental disadvantages:
1. With video surveillance it cannot be determined whether or not the vehicle is equipped with EETS OBE and who the EETS provider is[28].
2. If the compliance of the account cannot be checked on the spot a vehicle may have left the country before any violation has been noticed.

Real-time freezing[29], which allows for on-the-spot compliance checking can remedy this problem[30].

2.3.2 Real-time freezing

With real-time freezing, an account will be frozen each time a new record is added to this account[31]. By doing so, the account can be inspected by a toll charger at any time.

First notice that real-time freezing with on-the-spot checking is only useful for the on-board data. For data processing with the central equipment of the EETS provider, the value of real-time freezing is less obvious, if useful at all[32].

Below it assumed that only the on-board account for declaration is frozen in real-time.

When an on-board account is real-time frozen, it might be interrogated on the spot without stopping the vehicle. This may be done from the roadside, from another mobile or with handheld equipment using DSRC or infrared. In either case the transaction used for the interrogation of the account is called a compliance checking transaction.

A toll charger should have confidence that the following conditions are met.
1. The account was frozen indeed before OBE could notice a checking attempt
2. The last record links up correctly to the previous ones.
3. The declaration is based on the same real-time frozen account he could check.
   I.e. the OBE cannot use two accounts: one to be checked and one for declarations.
4. 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[33].

If these conditions are met, a toll charger can trust the on-board account checked on-the-spot as much as if it was checked with freezing per declaration as dealt with in 2.2.

These four trust conditions are dealt with in the paragraphs below.

[27] Another techniques that might be considered is active infrared (where the vehicle is permanently transmitting his identification).
[28] Except when a white-list is used, i.e. a list with (at least) the registration number of all vehicle under a contract with an EETS provider.
[29] Other terms that have proposed are: immediate freezing and continually freezing.
[30] Real-time freezing by sending the toll charger the signed hash-code after each addition of a record to the declaration account is not considered here (it is assumed to be too costly).
[31] This may be accomplished e.g. by calculating a new hash-code over the previous one together with the new record.
[32] It would require real-time access to the EETS provider's central equipment under the same or equivalent condition as set out below for real-time freezing of the on-board account.
[33] Note that the OBE knows this last check when the onboard account for a declaration is drawn up.

2.3.3 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.

This fraudulent 'fixing' might e.g. be accomplish by retaining the freezing of relevant records till it is known whether they may became part of an interrogation, or not. If not, an incorrect record may be added. But when the OBE notices a DSRC beacon, it freezes correct records and the OBE will pass the check.

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[34].

However, to guarantee that the freezing of the onboard account takes long enough is not trivial.

Of course, one can build a sufficiently slow device. However, then it shall be sure that this slow device is actually used[35]. A solution is to use a device that is trusted by the EETS provider and all toll chargers and that signs the freezing hash code[36] with a sufficient delay[37,38]. Hereafter this is called signing with a delay and the component that performs this signing is called a trusted element (as in [3]).

Then this trusted element shall be used to sign the total onboard account for the next declaration each time the OBE adds a new record to this account. Remember that this account shall have the properties mentioned above in 2.1. When spot-checked, the OBE should show that the presence of the vehicle at that location has been accounted for and that the fee[39] has been properly included in the accumulated total fee up to that moment. The last property implies that the accumulated fee due for the declaration period shall be part of the response to a compliance checking transaction as well.

One way to create such a trusted element is to use a smart card loaded with a dedicated trusted function for signing with a delay that makes use of a dedicated key pair with a certificate from a trusted third party.

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

As only the last record is checked, one should be sure that this record links up correctly to the previous one. In other words, one should be sure that:

1. the last record is indeed linked to the previous one[40]
2. there are no 'holes' between two subsequent records[41].

[34] In order to deal with very slow traffic, i.e. when there is more time to respond, one may require always a sufficiently fast response and measure any passing of such a threshold.
[35] If such a slow device would be used naïve, it might be possible to by-pass it with a fast one.
[36] Of course, the hash code may then also be calculated with that trusted device.
[37] What matters is that the time between two signing operations is more time than the maximum response time allowed for a compliance checking transaction. In other words the signature may be produced fast as long as there is enough time between two successive signatures.
[38] Hereafter this is called signing with a delay. Other terms coined are delayed signing, gradual signing, sluggish signing, slow signing, and temporised signing.
[39] Or any other total like distance driven, time spent, or number of passages.
[40] To be precise, each record should then account for both the last part of the itinerary and the correct inclusion of the fee for this part into the declared fee (see section 2.1, paragraph 2, item 2 and 3)
[41] However note that if the OBE should produce a record any minute, the record to be used for check cannot be more than one minute old (plus some time need for signing with a delay etc). This may limit the possibilities for fraud with holes considerably (say to a few percent).

With respect to the second point
This point deals with the possibility that the OBE may 'forget' a part of the itinerary between two subsequent records.

However this problem can be avoided easily by using records with accumulated values for fees, distances, etc., and by providing the checking equipment with the last two real-time frozen records instead of only the last one[42].

Note that this implies that even a thin OBE[43] should be capable of calculating an accumulated value relating to the fee due[44]. For distance related fees this may be the distance driven according to his (GNSS) sensor(s)[45].

With respect to the first point
This point deals with the possibility that the last records (or the last two records) are not properly linked to the previous ones. In the case where only the last two records are checked, the OBE may be able to produce pairs of records that reflect the last part of the itinerary correctly but not the earlier part.

This can be remedied by augmenting on-the-spot checking with checking of the complete declaration account after the declaration has been received.

Another solution is to rely on the trusted element. First note that the fraud as described above is only beneficial if the accumulated fee[46] in some record that is signed by the TE is lower than the accumulated value in the previous record. A TE can detect this.

Second solution may exploit time stamps. Suppose the OBE has produced two records A and B accounting correctly for the last part of the itinerary. In case the OBE should wants to produce a new fraudulent record D that takes the next part of the itinerary correctly into account but not the history, i.e. not the two previous records A and B, it has to produce also a fraudulent record C that can be used as the predecessor of D in case of an on-the-spot check. However, in that case the time-stamp for B and C will be the same (or almost the same) but significantly less then the regular period between two subsequent records. A TE can detect this[47].

To summarize, a toll charger can be sure that the last record that is frozen in real-time links up correctly to the previous records if:
1. a record contains accumulated values (instead of increments relative to the previous one)
2. an on-the-spot check provides him with the last two on-the-spot frozen records
3. the TE also signals a negative increment of the accumulated value[48,49]

[42] In that case the itinerary for last record starts always by definition at the end of the itinerary of the previous record..
[43] See also section 2.3.7.
[44] Although this is still for further study, a monotonic relation between this accumulated value and the fee due might be required. I.e. a greater fee is based on a greater value but not necessarily not vice versa.
[45] This distance may be amended then later on by map-matching algorithms etc. in the EETS provider's central equipment.
[46] Or any other total like distance driven, time spent, or number of passages
[47] Alternatively one might rely on sequence numbers, either generated or checked by the TE. But only if the exact number of records in the on-board account for a declaration can be checked as well, e.g. when a sequence number represents an exact period of time. (If not, a fraudulent C record might be inserted without being noticed).
[48] Depending of the onboard account, an accumulated value might be a fee due, a distance driven (in case of a fee per km), a number of passages (in case of a fee per passage), or a time spent (in case of a fee per unit of time).
[49] The TE should add then its checks (whether or not there was a negative increment and, if used, the minimum period between two subsequent time-stamps) to each record before is signs this record with the appropriate delay.

In addition the TE may also be required to report the minimum period between two subsequent time stamps. And, if this value is significantly lower than the agreed regular reporting period, this is also an indication for a defect in linking up previous records.

2.3.5 Trust that the declaration is based also in the checked account

With real time freezing, a compliance checking transaction can be used to check whether or not there exists an onboard account that passes the test.

However, the OBE may keep two accounts[50], one for the compliance checking transactions and one for the declarations.

To prevent this, firstly it should be required that the declaration shall be signed by the trusted element with the same key as used for real-time freezing. This prevents the use of two trusted elements.

Secondly, one might check that a declared accumulated value is not less than the value at the time the vehicle was checked[51]. Or, to be more precise, the declared accumulated value should be at least the value as reported by the OBE with the last on-the-spot check in the declaration period.

Note that this check requires a toll charger to store the following data from the most recent record received as the result of a compliance checking transaction: an identifier, the time, a hash code[52] over the location data, and the accumulated value.

2.3.6 Trust that the declaration is also correct after the last check

With real-time freezing there is a gap between the last check and the declaration. That gap is known by the EETS provider's equipment when the declaration is drawn up and is send to the toll charger.

So, instead of using the complete account, the OBE might attempt to base the onboard account for a declaration on the account that was frozen at the time of the last check (pretending the vehicle was not used afterwards).

However, as the vehicle was still vulnerable to be checked in this period, it should have kept an account and frozen it in real-time over this period as well. As this frozen account contains totals (we should not restart counting for every declaration period) and time stamps, it can be shown that it not possible not to declare for this period. The next declaration will be always linked up correctly to the preceding one[53].

2.3.7 Post-processing in the EETS provider's central equipment

An EETS provider may choose to equip the vehicle with simple OBE (also called thin OBE) and decide to use his central equipment to producing declarations based on the raw data provided by the OBE.

[50] And may even use separate trusted elements for these different accounts.
[51] At least in theory, the vehicle might not been uses any further between the check and the end of the declaration period.
[52] The location data is only needed on the spot and does not need to be stored. Therefore, it suffices to sign only the hash code for the location data, in order to make it incontestable in case it would not be correct. The location data self can then be deleted once it has been found correct by the compliance checking equipment.
[53] The declared fee is always the accumulated fee in the last declaration minus the one in the previous declaration.

As stated above, in such a case real-time freezing only applied to the on-board account (see 2.3.2) and the OBE should at least be capable of calculating a accumulated value (e.g. the distance driven) related to the fee (see 2.3.4, second point).

For his trust in the post-processing of the OBE date in the EETS provider's central equipment, a toll charger may relay on freezing per declaration in conjunction with unobtrusive observations[54].

2.3.8 Variations, details and trade-offs

2.3.8.1 Skipping periods for which no fee is due

As for freezing per declaration (see 2.2.5.4), periods for which no fee is due may be omitted with real-time freezing as well, e.g. when the vehicle is not used or used outside the toll domain.

2.3.8.2 The granularity of the onboard account

Except for the minimum period between two successive records (which should be longer then time needed for freezing with a delay), the reasoning used for an account that is frozen per declaration applies (see 2.2.5.2).

2.3.8.3 Using a universal TE for several types of accounts

Note the meaning of a counter is immaterial for the TE. It only has to check whether its value is decreasing or not. In case multiple counters are needed, only the OBE, the central equipment and the compliance checking equipment have to know which counter is used for which purpose. So, although this should be part of the context data, it is immaterial for the TE.

In case multiple counters are needed, each new record that is to be frozen has to contain for each of these counters the accumulated value.

2.3.8.4 Tariffs based on the length of stay with a (daily) ceiling

As for freezing per declaration (see 2.2.5.7), real-time freezing can be used for all kinds of tariff schemes.

E.g., a tariff for the length of stay with a daily limit can be supported with two counters, one for the accumulated total fee and one for the accumulated fee at the end of the previous day. In this way the compliance checking equipment can then detect whether the daily ceiling has been reached or not[55] and, consequently, whether or not the OBE is correct in (not) incrementing further the accumulated total fee at a certain time in a particular day.

2.3.9 Summarizing real-time freezing

As shown real-time freezing with on-the-spot checks can provide the same level of trust for an onboard account as freezing per declaration for which the checks are to be performed after the declaration with the hash code has been received.

However, in order to obtain this level of trust:

[54] In this case it might be worthwhile for efficiency reasons to use a dual 'aggregation structure' (see the examples in 2.2.5.4). I.e. one for real-time freezing (example 3 in 2.2.5.4) and one optimised for the freezing per declaration.
[55] The daily fee equals the accumulated total fee minus the accumulated fee at the end of the previous day.

1. The real-time freezing shall be performed with a trusted element (TE) that signs the account with an adequate delay
2. At least the last two frozen records are submitted to compliance checking equipment
3. Each record in the onboard account contains for each counter involved the accumulated value.
4. The TE shall be capable of signalling any decrease of the value of a counter.
5. The toll chargers checks the signed data obtained from his last compliance checking transaction with the declaration received from the EETS provider (see 2.3.5).

To conclude, real-time freezing of an onboard can be used for secure monitoring of this account if the five conditions above are fulfilled.

2.3.10 Freezing per declaration versus real-time freezing: the differences

Major differences between freezing per declaration and real-time freezing with on-the-spot checking are the following:

1. With freezing per declaration a toll charger has to store more privacy sensitive data over a given period (i.e. till the declaration is received):
   a. With freezing per declaration he has to store observed time/location details for a vehicle
   b. With real-time freezing he has to store only the time and the accumulated fee
2. With freezing per declaration a toll charger needs only a video camera instead of an expensive DSRC beacon with a video camera for real-time freezing.
3. With real-time freezing the onboard account can be checked directly and, if not correct, the vehicle can be stopped on the spot. (With freezing per declaration the vehicle might have left the country in the mean time)
4. Real-time freezing only makes sense for the onboard account, not for any additional processing of the OBE data with the central equipment of an EETS provider. For the latter freezing per declaration should be used. However, processing location data with the EETS provider's central equipment is less privacy friendly than processing this inside the OBE.

However, it should be noted that with real-time freeing a toll charger could also combine both type of checks: on the spot checks and checks for unobtrusive observations after he has received the declaration (e.g. to check any central processing performed by the EETS provider).

2.4 Additional checks for secure monitoring with a trusted element

When used for secure monitoring with real-time freezing, it is worthwhile to consider whether there exists any additional security measures that can be implement with a TE. When the TE is fabricated in large numbers, those additional features that might increase trust may be available without adding significantly to the cost.

Note that for real-time freezing of an onboard account the OBE has to deal with a stream of records that contain time and location data as well as counters. In [4] it has been proposed to pass this complete stream of data to the TE. This is not only for the calculation of the hash-code and the signature, but also to perform some elementary checks on this stream of records, including the following:

1. The minimum and maximum increment of a sequence number in the successive records A value different from one indicates deviant OBE behaviour.

2. The minimum and maximum of the elapsed time between the time stamps in successively monitored records.
   A negative minimum or very small value indicates deviant OBE behaviour.

3. The maximum distance between the locations recorded in successive records.
   Which may be not exceed a certain value under a particular toll regime

4. The minimum and maximum distance driven between to successive records
   Which may be not exceed a certain value under a particular toll regime

5. The minimum value of item 4. minus item 3.
   A negative minimum may indicate deviant OBE behaviour. However, the vehicle may have been carried by e.g. a ferry, a train or another vehicle.

6. The maximum of the 'minimal speed' based on the time and location as recorded in successive records.
   Which should not exceed some (vehicle dependent) threshold

7. The maximum of the average speed based on the time and the distance driven as recorded in successive records.
   Which should not exceed some (vehicle dependent) threshold

8. For each counter, the minimum and maximum value of the increment between two successive updates this counter.
   A negative value may indicate deviant OBE behaviour.

   Note that signalling of a negative increment is required also for real-time freezing.

9. For a counter, the minimum and maximum value of the increment per km and the increment per hour between two records updating this counter.
   Which shall be within the limits of the fee as determined by the tariff scheme.

It should be noted that these measure are additional. As explained in section 2.2 – 2.3 a toll charger can readily check whether or not the observed presence of a vehicle is accounted for and in correctly included in the total fee. Nevertheless, when one or more of these additional measures are implemented, a toll charger may consider reducing his roadside surveillance efforts.

The question whether or not it is worthwhile to implement one or more of these additional checks is left to the EETS provider and/or toll chargers.

Note that if these additional measures are implemented their values shall be calculated and signed by the trusted element as introduced in section 2.3.3, i.e. with a device that is trusted by the toll chargers.

3. Additional security related issues

3.1.1 The toll account certificate

In principle a messages from an EETS provider to a toll charger shall be signed by, or on behalf of, the EETS provider.

In case of a declaration it shall also identify the vehicle for which the toll is due, and, preferably, the toll account number (TAN)[56] that identifies both the EETS provider (as the issuer of the account) and their client[57].

The vehicle should be identified by its registration number. This allows roadside equipment used for compliance checking transactions to compare this number with the result of an ANPR (Automatic Number Plate Recognition)[58].

The TE used by the EETS provider for the vehicle shall be identified as well. Not to confirm that some element can be trusted (this is addressed in 3.1.2), but only to confirm that the EETS provider is using a particular TE for a particular vehicle.

In principle, the identity of the OBE is not of any value for the toll charger[59].

To sum up, the above can be accomplished with a toll account certificate (TAC) that is signed by the EETS provider and that associates the following basic elements:
1. an identifier (and the public key) for the TE[60]
2. the public key for the verification of OBE signatures[61]
3. the vehicle's registration number
4. the TAN

For the storage of a toll account certificate there are no onerous requirements.

Potential corruption of the private key used for OBE signatures may be dealt with in two ways:
1. the security of this key may be safeguarded with requirements for the certification of OBE
2. the EETS provider is simply held responsible for this key (i.e. for its own security)

The first case might look appealing but then these requirements, if mandatory, should be part of a decision of the Commission. Consequently, it would allow an EETS provider deny (part of) its responsibility when using his certified OBE. Therefore, the second case is preferred.

[56] In DSRC based systems this TAN is called a Personal Account Number (PAN). See ISO 14906 and CEN 15906.
[57] As the EETS provider should pay the toll to the toll charger, a declaration should at least identify the EETS provider. For practical reasons the users account should be identified as well. If not, parties have to relay solely on sometimes exotic and not always unambiguous registration numbers.
[58] In theory one can obtain the registration number of the vehicle with an OBE also with a request to the EETS provider. However, would require quite some communications overhead and that the EETS provider can answer those request on a 7*23 hour basis. Moreover, it would violate the privacy of the user as this check would not exhibit to the presence of the vehicle in a particular toll domain / country to the EETS provider.
[59] If needed, it could be obtained from the EETS provider for a known TAN.
[60] At a first glance, the EETS provider may use the TE also for OBE signatures on his behalf. And if so, the certificate may contain only the value of the public for the verification of the TE signatures.
[61] Which may the same as the key for by the TE for signing with a delay, or another key stored on the TE or in the OBE.

3.1.2 The TE certificate (TEC)

As stated in 2.3.3, a trusted element should contain a certificate signed by the trusted third party (i.e. trusted by the EETS provider and the toll chargers). This TE certificate (TEC) associates the following basic elements:

1. the verification key to be used for TE signatures that are signed with a delay[62]
2. the TE number

For the storage of a TEC there are no onerous requirements.

3.1.3 The integrity status of the TE

Most modern smart cards contain sensors that can detect events that may have compromised the integrity of the TE. Common sensors are: low and high temperature, low and high supply voltage, and low and high clock frequency.

These the values of these sensors should be added to any data signed by the TE.

3.1.4 The status of the OBE

OBE may signal its user three values (e.g. lights): 1(e.g. green): okay, no action required; 2 (e.g. orange): operating okay in this toll domain, but needs maintenance in due time and might not operate correctly in another toll domain; and 3 (e.g. red): not operating correctly in this toll domain, immediate action required.

It would help[63], if the OBE would add to its response on a compliance checking transaction a flag, indicating whether its present status is red or not and, if red, the date and time when it turned red.

Of course, apart from this three-valued signal and flag, the OBE might need to inform the EETS with other details about its health.

3.1.5 The compliance checking transaction

As stated above the OBE should deliver the last two frozen record of the onboard account in response to a compliance checking transactions. Each record should then at least contain:

1. a time / location stamp,
2. for each counter in use:
   a. the accumulated value and
   b. a signal whether or not the value of a counter has been decreased.

In addition the response may have to contain:

1. the vehicle's tariff class under the various tariff schemes in the toll domain[64]
2. the vehicle's toll account certificate (TAC), see 3.1.1
   (which is independent of the toll domains)
3. The TE certificate (TEC)
   (to certify that the signature used is indeed the signature of a TE),
4. the OBE's status flag, see 3.1.4
5. The integrity status of the TE, see 3.1.3

[62] But may also be used for all other OBE signatures on behalf of the EETS provider.
[63] E.g. in resolving disputes between the EETS provider and the toll charger, and between the EETS provider and its user.
[64] If used in the on-board account this may be needed for the compliance checking equipment to check the fee calculations. If not used for the onboard account, it may nevertheless be used by the toll charger's compliance checking equipment/officer to check this class with the measured / visual appearance of the observed vehicle. In the latter case it should be checked the same class is used also by the EETS provider's central equipment for the declaration.

3.1.6 The confidentiality of a compliance checking transaction

For privacy reasons, the use of a compliance checking transaction should be restricted to authorised parties[65]. In more technical terms, the data provided by the OBE in response should be treated confidential. This confidentiality can be accomplished by encrypting the result[66].

Authorised entities should make themselves and their public keys[67] known to the EETS provider, who can load this data in his OBE.

When invoking a compliance checking transaction the checking equipment should add the entity identifier and a key identifier to the transaction's argument. Then the OBE can use this data to encrypt the result[68].

When the key should become corrupted, it should be revoked by the toll charger in due time.

And, when revoked by a toll charger, it might require quite some time for an EETS provider to update all his OBE[69].

3.1.7 Secure monitoring versus a tamper proof OBE

As already stated in the introduction, secure monitoring starts with the protection of the data, not with the protection of OBE, e.g. by making the OBE tamper-proof.

Both methods are orthogonal. Secure monitoring does not add to a tamper proof OBE and does not require a tamper proof OBE (although real-time freezing needs a tamper-proof TE). Conversely, a tamper proof OBE does not add to secure monitoring and does not require secure monitoring.

An advantage of secure monitoring is that the requirements can be clearly specified and tested for a particular implementation. Requirements for tamper proof OBE are much more difficult to specify. One has to deal with mechanical impact, electromagnetic impact, the impact of temperature, moisture, supply power faults etc. Also one has to deal with what is needed for an inspection: the human eye, a trained inspector, a magnifying glass, infrared or other light, and/or measurement of the OBE's power consumption, etc.

Secure monitoring will be probably less costly. Apart for the TE, it can be implemented in software and the software development cost can be divided over all products[70]. The cost of a tamper proof OBE will directly add to each OBE and this might be much more the cost of a TE.

[65] If not third parties would be able the use this transaction tot trace a vehicle and, eventually, to trigger an attack when a particular vehicle is detected.
[66] An alternatrive approach would be to control the access to this data by requiring authentication of the compliance checking equipment. However, as can demonstrated easily, encryption provides more security, can be more efficiemtly implemented, and is there more suitable for a compliance checking transaction that has to be executed in a short time.
[67] The usual instrument is a trust certificate.
[68] Due to speed constraints the result should be pre-encrypted with a secret transaction key generated by the OBE. Then the OBE only has to encrypt this secret key with the correct public key and the encrypted key to the pre-encrypted result.
[69] Note that for technical reasons an EETS provider cannot contact OBE but has to wait till the OBE contacts him. The latter depends on his update policy and is outside the scope of this paper.
[70] Processing power and storage are rather cheap nowadays and it might turn out that, apart from the TE, secure monitor can be implemented by using the spare capacity of devices that would be present anyway.

Nevertheless, secure monitoring depends on the possibility to observe the circulation of a vehicle in a toll domain. For areas where the circulation of vehicle will not be observed, if significant, one may rely on 'tamper proof' OBE.

4. Glossary and abbreviations

4.1 Glossary

Declaration
Short for Toll declaration

Declaration account
The account that underlies a toll declaration

NOTE: The toll account assumed to contain the vehicle's itinerary in the declaration period and the calculation of the fee due for this itinerary. The account is not included in the declaration that is send to the toll charger.

EETS Provider
A legal entity providing to its uses toll services on the EETS toll domains.

EETS User
See User

European Electronic Toll Service (EETS)
A service which allows users to circulate a vehicle in all the toll domains falling under the scope of Directive 2004/52/EC and pay the corresponding tolls with a single contract and a single on-board equipment.

Freezing per declaration
Freezing of a declaration account when the declaration is drawn up and signed.

Non-repudiation
The property that non of the parties involved in a communication can deny in all or in part its participation in the communication[71].

On-board equipment (OBE)
A complete set of hardware and software components required for providing EETS which is installed on board of a vehicle in order to collect, store, process and remotely receive/transmit data.

Secure monitoring
A service that allows a toll charger to check whether or not the observed presence of a vehicle has been correctly accounted for by the EETS provider.

Signing with a delay
A signing operation that requires more time than the maximum response-time allowed for a compliance checking transaction[72].

[71] Adapted from ISO 7498-2 [9].
[72] Say, e.g., one second

Toll charger
a public or private organisation in charge of levying toll for the circulation of vehicles in a toll domain.

Toll declaration
a statement to a Toll Charger that confirms the circulation of a vehicle in a toll domain in a format agreed between the Toll Service Provider and the Toll Charger.

Toll domain
an area of EU territory, a part of the European road network or a structure such as a tunnel, a bridge or a ferry where a toll regime is applied.

Toll regime
a set of rules, including enforcement rules, governing the collection of toll in a toll domain;

Tolled object
A distinguished part of a toll domain for which one or more tariff scheme applies.

Examples: A bridge, a tunnel, a ferry or a stretch of a road.

Trusted element (TE)
A onboard component that is trusted by the EETS provider and all the toll chargers and suited for real-time freezing.

Examples: One might think of a small size smart card that is issued by a trusted third party.

Trusted element certificate (TEC)
A certificate signed that by a trusted third party to certify that a particular key is used by a particular TE.

User
a (legal) person who subscribes a contract with an EETS Provider in order to have access to EETS

Vehicle tariff class
A class of vehicles for which the same toll is due when driving at the same time the same itinerary[73].

4.2 Abbreviations

CE	Central Equipment
DSRC	Dedicated Short Range Communication
EETS	European Electronic Toll Service
GNSS	Global Navigation Satellite System
OBE	On Board Equipment
TAC	Toll Account Certificate
TAN	Toll Account Number
TE	Trusted Element
TEC	Trusted Element Certificate

[73] In mathematical terms for each two vehicles in this class should have to pay the same toll when

5. References

[1] 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://ww.tipsystems.nl)

[2] 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%20Groups/EG%207%20rapport%20final%2017%20octobre%202006.pdf

[3] 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%2012%20Final%20Report%20v1.0%205apr07.pdf

[4] Annex C of Draft ISO/PDTS 17575-3, Road transport and traffic telematics — Electronic fee collection — Application interface definition for electronic fee collection (EFC) based on Global Navigation Satellite Systems and Cellular Network (GNSS/CN) — Part 3: Provisions for updating On-Board Equipment (OBE), February 10th, 2008. Available via http://www.xs4all.nl/~visjpmm/papers/Secure%20monitoring%20-%20History/Draft%20TS%2017575-3%20-%2020080208%20-%20Annex%20C%20-%20Compliance%20checking%20provisions.pdf)

[5] 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

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

[7] ISO/IEC 10118-3:2004, Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[8] FIPS 180-2, Federal Information, Processing Standards Publication 180-2, Specifications for the SECURE HASH STANDARD, 2002 August 1, amended 25 February 2004.

[9] ISO/IEC 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[10] See for an early presentation and a early paper: http://www.xs4all.nl/~visjpmm/papers/Secure%20monitoring%20-%20History/summary.html