

Electronic payment and control functions in the BESTYR project

Master Thesis by Ulrik Karlsson

2000-03-30 for SWECO ITS

Abstract

This master thesis aims at developing to a demonstrate system for road-pricing. Road-pricing should in this context be interpreted as motor vehicles being charged a fee based primarily on location and distance driven. It thus provides a way of internalising environmental costs in accordance with the “polluter pays”-principle. The demonstration system should be used as a starting point for discussion of road-pricing by the general public.

A GPS-receiver is used for positioning and a GSM cellular-phone for communication. The demonstration system is programmed in Java. Several cryptographic techniques such as symmetric and asymmetric encryption and digital signatures are put to use.

All interactions in the system take place between four actors: the vehicle, the commerce server, the charging authority and the observer. The vehicle makes anonymous payments to the government through the commerce server. Observing the vehicle and asking for the receipt that proves correct payment ensures compliance with the system.

Modular system design and awareness of personal integrity have been emphasised.

The report and the demonstration system have not found any problems or weaknesses that makes α -BESTYR impossible to implement.

Contents

1	Introduction	1
1.1	Problem description	1
1.2	Requirements	2
1.2.1	Integrity	2
1.2.2	Security	3
1.2.3	Reliability	4
2	Background	5
2.1	Political	5
2.2	Road-pricing	5
2.3	Cryptography	6
2.3.1	Symmetric cryptography	6
2.3.2	Asymmetric cryptography	6
2.4	GSM Security	7
2.5	GPRS	7
3	System	8
3.1	Overview	8
3.2	Hardware	9
3.3	Information flow	10
3.3.1	Initialisation procedure	10
3.3.2	Payment procedure	10
3.3.3	Compliance check procedure	11
3.4	Components and objects of the vehicle	12
3.4.1	gpsReceiver and clock	13
3.4.2	taximeter and feeMap	13
3.4.3	cryptographer	13
3.4.4	Random-number-generator	15
3.4.5	verifier and storage	15
3.4.6	communicator	16
3.4.7	Licence plate	16
3.5	The commerce server	16
3.6	The observer	17
3.7	Components and objects of the charging authority	18
3.7.1	communicator and storage	18
3.7.2	requester and idipRegister	18
3.7.3	verifier, controller and aberrationReport	18
4	Compliance check	19
4.1	Observers	19
4.2	Time delay	19
4.3	Checkpoints	19
4.4	Who pays?	20
5	Security	21
5.1	A virtual control zone	21
5.2	Algorithms and key lengths used	21
5.3	Cryptographic attacks	21
5.3.1	Exhaustive search	22
5.3.2	Physical attacks	22
5.3.3	Passive attacks	22
5.3.4	Active attacks	22
5.4	Does a-BESTYR fulfil the security requirements?	23
6	Personal integrity	25
6.1	Cameras	25

6.2	Receipts	26
6.3	Monitoring of the cellular phone radio-frequencies	26
6.4	Base station triangulation	26
7	Paying outside a-BESTYR	27
7.1	Advance payments	27
7.2	GSM positioning	27
8	Conclusion	28
9	Further work	29
10	List of abbreviations	30
11	Appendix	31
11.1	IP-addresses	31
11.2	The NMEA-protcol	31
12	References	32

1 Introduction

Most people will agree that objectivity when building or describing a system of any kind is very hard, if not impossible, to achieve. With this in mind I think that my personal motivation is important to know. Below I will describe why for my master thesis I chose to work with the system architecture and implementation of an automatic road-pricing system.

I see the environmental problems as one of the more pressing issues of today. But the problems of today are different from those of the seventies or the eighties since the polluter no longer is a big company or organisation of some kind but the accumulated effect of many small actors. The prime example being CO₂ emissions from vehicles running on fossil fuels. This is the problem my master thesis project will address. I think that the way to tackle CO₂ emissions from vehicles is a strict “polluter pays” approach, the concept of road-pricing, charging a fee for motor vehicles based primarily on location and distance driven, seems to offer exactly this.

A lot has been written about road-pricing, in this context to be interpreted as motor vehicles being charged a fee based primarily on location and distance driven, but surprisingly few systems have actually been implemented. Systems including a GPS-receiver for positioning and mobile telephony communications such as GSM are especially rare. The cities of Oslo and Singapore have relatively recently introduced road-tolls and represent two of the most advanced systems today. Neither of them includes GPS or mobile communications. Another example is the ROBIN-system¹ that soon will be running in Germany to toll trucks. It includes a GPS for positioning but relies on DSRC (Dedicated Short Range Communications). One reason for this slow development is no doubt the fear of violating personal integrity. This threat is both real and unreal and will be further discussed in chapter 6. My conviction however, is that if the ideas are to be understood and discussed by the general public it is crucial that a demonstration system is built.

This master thesis project constitutes the first phase of BESTYR (Betalning av miljöstyrande avgifter för bilar, Payment of Environmental Fees for Cars) which is a project to take care of the technical solutions for the Swedish part of the PROGRESS (Pricing Road Use for Greater Responsibility, Efficiency and Sustainability in Cities) project. PROGRESS is a project financed by the EU (DG Transport) and the Swedish National Road Administration to examine road-pricing. Eight cities in the European Union are currently participating in PROGRESS, which is a project that studies different aspects of road-pricing. The city of Gothenburg is the Swedish participant. The BESTYR-project deals with the technical solution of the Swedish PROGRESS-project.

1.1 Problem description

The aim of BESTYR is set to produce a solution that can bill the vehicle owner a fee computed from driven distance times price per kilometre. The kilometre price will vary depending on position, time and identity of vehicle and owner. The identity is an aggregate that reflects static parameters tied to vehicle or owner such as environmental performance or taxed income. Mathematically the fee can be expressed as:

F = fee	f = fee function
R =driven route	\bar{p} = position
T = time	i = aggregate reflecting for example environmental performance and taxed income

$$F = \int_R f(\bar{p}, t, i) d\bar{p}$$

The solution will be used for illustration of ideas and as a starting-point for further discussion and the emphasis will fall on the whole rather than the details. This will allow some ad hoc decisions. The first attempt at a demonstration system is called α -BESTYR and together with this report constitutes my master thesis project.

1.2 Requirements

A number of requirements have to be met in order to successfully implement the final BESTYR-system. It is a fair guess that user acceptance, legislation and politics will present the most complex problems. However, most of them fall outside the scope of this report. The requirements on α -BESTYR will be presented under three different headings. A common requirement for integrity and security is that they should rely not on the hardware components, but rather on the communication protocols and known, widely evaluated cryptography-algorithms. That is, trust in α -BESTYR requires only trust in the protocols and algorithms used. Today there are, especially for trucks, many different ways of charging for road-use for example paying at a both in a toll station or buying a pass for a certain time period. A requirement of the system as a whole is that it must be able to function in parallel with other modes of payment.

1.2.1 Integrity

To carefully safeguard personal integrity is not only a moral obligation but also a political one. Critics of road-pricing fear constant surveillance of drivers. Since road-pricing is generally a very political issue, the ability to satisfy the political opinion is a case of do or die.

It is hard to achieve the ideal solution where making payments and ensuring that the user is in compliance with the system can be totally anonymous processes. One might even argue that compliance check is impossible if the user is totally anonymous. (Who is responsible in the case of non-compliance?) This situation has been recognised by the ADEPT (Automatic Debiting and Electronic Payment for Transport) project and α -BESTYR will use a formulation from there: "As far as service provision and the payment mode allow, the actions of the user should be anonymous."² A second requirement on the system will be that it, as far as possible allows the user to choose between different providers of the services that involve personal information (banking and communication).

1.2.2 Security

The discussion around road-pricing and security issues has been extensive. If the system is not quite safe then it will quickly be undermined. Several checklists have been produced. I will present some of the items that are relevant to BESTYR.

From the report "Stockholm Integrated Payment System"³:

Segment integrity	By tampering system parts (=segments), functionality and data could be disclosed or changed; segment integrity defines the difficulty of tampering a device.
Message integrity	By changing the contents of messages, its meaning would be changed; message integrity defines the difficulty of changing its contents by unauthorised entities without being noticed.
Entity authentication	By entity authentication the correctness of the entity identity is proven.
Message authentication	By message authentication the correctness of the origin (originator/sender/creator) of the message is proven.
Message timeliness	By message timeliness the correctness of the message time stamp is proven.
Non-repudiation	Confirmation of submission, delivery or receipt of messages.
Accountability & audit	Accountability is the property that an entity may be held responsible for its actions so that violations of system security may be traced uniquely to it.

From "Security: threat analysis and proposals for security algorithms"⁴:

Confidentiality	Addresses the disclosure of message contents to unauthorised entities.
-----------------	--

From "Why do we need Public Key Cryptographic Solutions in the form of 'Slow and Fast Charge' in open Integrated Payment Systems for ADS"⁵:

The user should be able to convince himself/herself of the legitimacy of collection and charging equipment and operators.
The user should be able to convince himself/herself (and others) that balances cq. Service rights are properly set/increased/decreased.

System malfunctioning not due to his/her own handling should have no financial consequences for him/her personally.

1.2.3 Reliability

The reliability of BESTYR is essential for acceptance and thereby also compliance. α -BESTYR should therefore be based on existing techniques. It should also be highly modular in order to allow for updates and revision. It is wise to remember that going through a number of well-defined transactions with 100 actors is one thing and doing the same thing with 4 million actors, is something entirely different.

2 Background

2.1 Political

The current situation in Sweden for a road-pricing scheme such as BESTYR is well described by Jonas Sundberg (my translation)⁶:

Society has in several contexts expressed the need to use road-pricing schemes to be able to influence the spatial and temporal distribution of big city traffic. This has recently been expressed by the (Swedish) government in a transport political proposition, as well as by the EU through the Green (White) Paper on Fair and Efficient Pricing. An outline of such a system was developed for the transport political investigation and was a part of their final report. This outline was met with extensive criticism. It was said that the “proposal” was incomplete; how are temporary visitors handled? How will payment control be carried out? Extensive criticism was also directed towards the use of GPS for positioning of vehicles with gave rise to expressions such as “space police”, for integrity infringement. The question has been studied internationally in a similar mode, most recently in Copenhagen but also in for example Zurich, Lyon and London. The question has also reappeared in Hong Kong. The Swedish National Road Administration has just finished a study regarding transport demand management for environmental control. Legislation is expected after a proposition in the Swedish parliament.

Since then the debate has continued, perhaps most notably with an article by Minister for the Environment Kjell Larsson, in Dagens Nyheter⁷. It provoked much debate and resulted in several replies in the same newspaper^{8,9}.

2.2 Road-pricing

The use of a road-pricing scheme has two facets. It provides a source of revenue that can be used to finance better roads and public transportation. But it will also act as a far more sensitive political instrument for traffic- and pollution-control than the fuel tax of today. A high fee per distance can keep cars away from areas with much traffic congestion and thereby reducing health risks and give public transportation more road-space. At the same time transport in less populated areas will not be affected at all. The advantage of road-pricing over more approximate solutions such as car tax, fuel tax or road tolls is that their crudeness produce a number of charging situations that are perceived as unfair. This makes them hard to implement for political reasons.

There are many parameters that *could* be used for pricing the access to roads. But simplicity is of utmost importance. A simple system keeps the maintenance costs down and is easier for the users to accept. No system will be seen as fair, or will alter any behaviour patterns for that matter, if the general public can not understand it. Some of the factors that could be used are position, time of day and environmental classification of vehicle.

Furthermore there have been concerns that road-pricing will turn driving into a “class issue”. Swedish conservative politicians Carl Cederschiöld and Sten Nordin write (my translation):

“The fees have as their sole purpose to force people with ordinary incomes not to use their cars”¹⁰. Incorporating taxed income as a parameter when computing the fee and thus making it progressive can be a solution. Special exceptions could also be made for people with certain occupations, people with physical handicaps, etc.

2.3 Cryptography

Cryptography is an old art that has made significant advances in recent years. The 2nd World War could be seen as a starting point for a more widespread use. The most famous example no doubt is the German Enigma-machine. Cryptoanalysts in Bletchley Park England, USA and Poland worked hard and successfully to break this code. In Sweden professor Arne Beurling managed to decipher codes from another cryptographic machine, the Geheimschreiber, with only the help of printouts of the actual traffic, an amazing feat.

The codes of the Enigma and the Geheimschreiber are relatively easy to break with the help of modern computers, but advances made in the USA in the seventies form the cryptologic building blocks we still use today. The National Bureau of Standards (now the National Institute of Standards and Technology) proposed the Data Encryption Standard developed by IBM to be a federal standard. It was adopted in 1976 and is still one of the major symmetric ciphers. 1976 was also the year when Whitfield Diffie and Martin Hellman published their paper “New Directions in Cryptography” on asymmetric ciphers (also independently discovered by Ralph Merkle).¹¹

2.3.1 Symmetric cryptography

Symmetric or secret-key cryptography is what most people understand as cryptography. A cipher-algorithm together with a key is used to obscure plaintext into ciphertext. To retrieve the plaintext from the ciphertext one uses the inverse of the cipher-algorithm and the same secret key. Unlike with asymmetric cryptography, the inverse function is easy to compute if the key is known. Normally, the algorithm is not kept secret; the secrecy rests in the key.

2.3.2 Asymmetric cryptography

Asymmetric or public-key cryptography instead uses two keys, one public and one private. To encrypt plaintext one would use the intended recipient’s public key. To decipher one needs the private key which, as the name implies, is available only to the recipient. The encryption uses so-called “one-way functions” for example multiplying two very large primes or taking a discrete logarithm. The name “one-way” is used since it is very hard to invert them.

Asymmetric cryptography also has a very important application in digital signatures. The basic idea is to encipher the plaintext that is to be signed with the signer’s *private* key. The public key, which is available to everyone, is used to decipher. If the ciphertext have been changed the deciphering will fail to produce anything readable.

Asymmetric and symmetric cryptography also differs in performance. Asymmetric encryption is much slower and generally produces larger cryptotext (this is the case with the algorithms used in α -BESTYR) than symmetric with comparable level of security. Also the keys used for

asymmetric crypto-systems are longer. In my work I will use a hybrid system that takes advantage of both asymmetric and symmetric cryptography.

2.4 GSM Security

What makes it necessary for BESTYR to develop its own cryptographic solutions? All communication is made over the GSM network which includes both authentication (which at least partly could substitute digital signatures) and encryption of the transferred data. Authentication in the GSM network is achieved through a shared secret that is embedded in the subscriber identity module (SIM) card and stored in a register at the telecom operator's. When the operator wants to ensure that the mobile unit that has made contact actually is whom it claims to be, it sends a challenge in the form of a random number. This number is encrypted with a symmetric algorithm using the shared secret as key. The result is then sent back. All the operator has to do is to compare this with an encryption it has made itself using the same shared secret as key.¹² In α -BESTYR I will not worry about authentication but trust that a scheme relying on the shared secret in the SIM-card can be implemented at a later stage. This scheme should involve authentication of both parties (instead of just the mobile unit as is the case in GSM authentication).

The data protection of GSM is inadequate for use in BESTYR. First of all it only provides encryption when the data is sent via radio waves from mobile unit to telephone operator. In other words all information is freely available to the telephone operator. Secondly the algorithm used to encrypt data, A5, is vulnerable to an exhaustive search (see section 5.3.1) since it requires only 2^{40} encryptions.¹³

2.5 GPRS

General Packet Radio Service (GPRS) is a mobile communication standard that can be put "on top of" the GSM standard. GPRS is designed for data-packets rather than voice-data. The difference is drastic. Instead of setting up a connection by dialling in to a server and then occupy the entire bandwidth during the call, GPRS is (seemingly) always online but only occupies bandwidth when sending a packet. It is much more resource efficient and enables cheaper and faster communication. The support for cryptographic protection is slightly stronger with GPRS, but still not enough for use in BESTYR.

It is worth to noting that the result from trying to send data to a mobile GPRS terminal that is switched off is not much different from trying to make a call to a cellular phone that has been switched off. Data in the GPRS case would simply be discarded with a system message saying that the terminal is unavailable. Or it could also be handled by an application on the server, putting it on a download queue that is transmitted next time the mobile unit makes itself visible to the network.

Trying to predict when GPRS will be introduced and how much it will cost, is guesswork. Agreements between net operators and cellular phone makers are being concluded today. The answers one would want are so far, business secrets. Some rough estimates can however be made. It has been mentioned in the general discussions that the introduction of GPRS will be sometime during 2000, in Sweden at the end of 2000 or in the beginning of 2001. The cost has been estimated to 10\$/Mb by officials at the telecom company Ericsson.^{14, 15}

3 System

3.1 Overview

α -BESTYR has four important actors. The information-exchange between the four deal with either payment for using the roads or compliance checks. The actors are:

- The vehicle
- Some kind of organisation (the `chargingAuthority`) that has been assigned the task of managing BESTYR
- A commerce server to deal with the payments (the `commerceServer`)
- An observer (i.e. the police, traffic wardens or video cameras mounted over busy roads) to get information that can be used to ensure compliance.

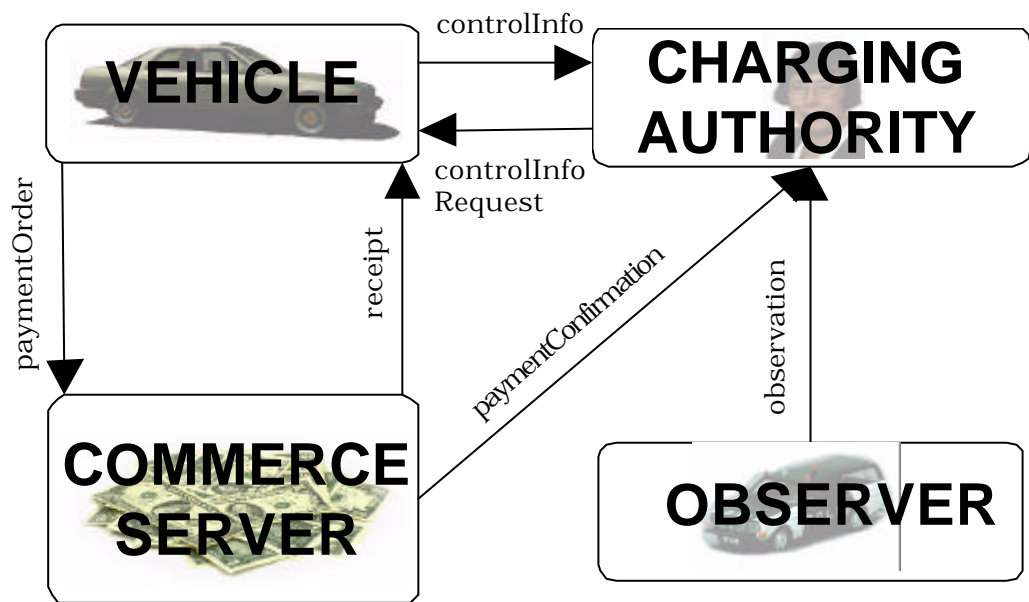


Figure 1. The four actors

The `vehicle` makes a continuous log of time and position and computes the fee that is to be paid. It then proceeds to make the payment through the `commerceServer` to the `chargingAuthority`. To prove successful completion of the procedure a `receipt` is returned to the `vehicle`. The `receipt` contains the corresponding part of the log. This concludes the payment.

When the `observer` makes an observation of the `vehicle` it is sent to the `chargingAuthority` who asks the `vehicle` for the corresponding `receipt`. The amount paid and the amount that should have been paid are compared. If there is a discrepancy between the two figures, this is registered. This concludes the compliance check procedure.

The described communication between the actors in the system is an example of an adjudicated⁶ communication protocol in that it normally maintains a high level of integrity. But if

the charging authority (or the vehicle owner) suspects cheating there is a body of data making it possible for a trusted third party, say a court, to determine if someone has cheated.

All information exchange between the vehicle and the other actors is made over channels that are considered insecure. To safeguard the integrity of the vehicle owner most of the information is enciphered.

3.2 Hardware

The vehicle unit in α -BESTYR contains a GPS-receiver for positioning, a mobile phone for communication and a Java virtual machine running cipher-algorithms and acting as the intelligence and glue of the system. Currently the operating system that runs the Java virtual machines is Microsoft Windows 98 on a Toshiba Libretto 50 CT laptop-computer. All the other actors are run on stationary computers with Windows NT 4.0. The choices of operating systems are likely to change in the future after an evaluation of possible alternatives.

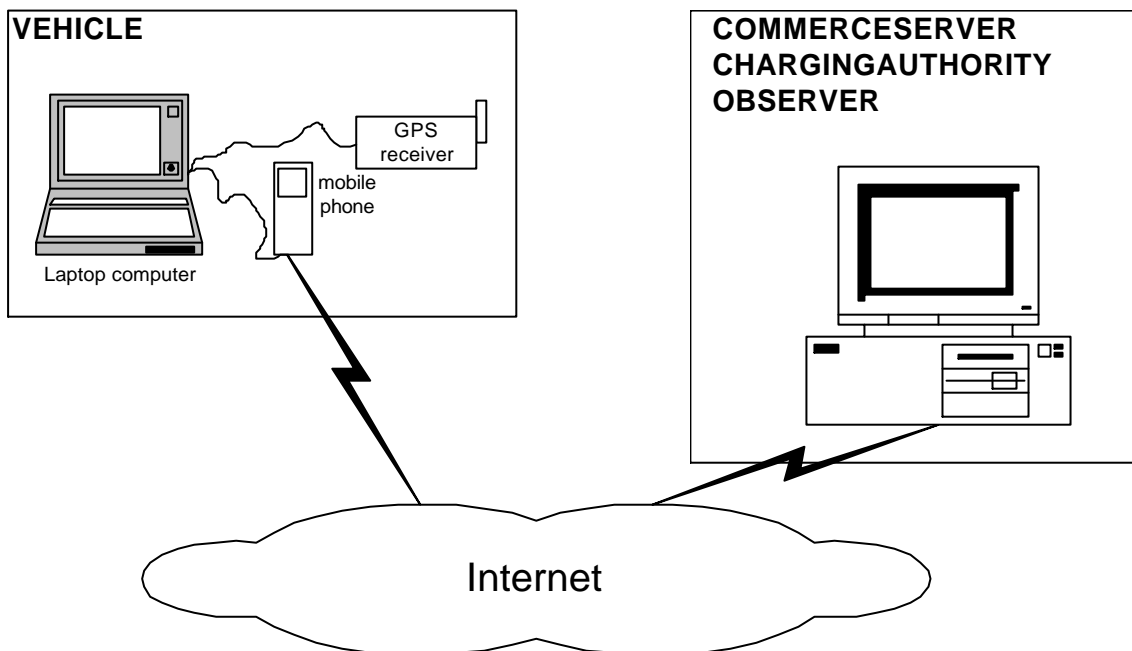


Figure 2. Hardware setup

I would like to point out that although I in this report have chosen not to elaborate on alternative positioning methods many are available, for example GLONASS, the Russian counterpart of GPS, or GSM positioning. Of course the GSM-positioning is the same as performing base station triangulation, which introduces integrity problems that are further discussed in chapter 6.

The nature of the BESTYR-system clearly indicates that packet based communications are the preferable choice, unfortunately it is not publicly available yet and so α -BESTYR will use a GSM mobile phone with built in modem. Both systems use the IP-protocol, which means that the difference in implementation is small; instead the difference lies in performance and cost. A modem connection is sufficient for the small demonstration of α -BESTYR.

The programming language Java was chosen because of its programmer friendliness, which allows for short development time, and its strong support for cryptography. Before the system is described in detail let's look at the information flows in it.

3.3 Information flow

3.3.1 Initialisation procedure

Before the actual road-pricing system can operate some pieces of information have to be shared. In α -BESTYR the `chargingAuthority`, `commerceServer` and `observer` all have statically allocated IP-addresses, they can therefore be put in a register in the `vehicle` when it is created. The `vehicle` on the other hand gets an IP-address that is dynamically allocated (see Appendix on IP-addresses section 11.1). The first step in the initialisation procedure is that the `vehicle` sends its IP-address to the other actors.

In the second step the public keys are shared. First the `vehicle` sends its public key to the `chargingAuthority` and the `commerceServer`. Then it waits until each of the other two has responded by sending their public keys. This procedure is purely a construction for the demonstration system and is open to attacks described in section 5.3.4 where I will also describe how it can be improved.

3.3.2 Payment procedure

The `vehicle` sends an information package called `payment-Order` to the `commerceServer` to initiate the payment procedure. The `payment-Order` contains the vehicle identity, the amount to be paid, the time-position log and a transaction identity. The vehicle identity and the amount to be paid are asymmetrically encrypted with the `commerceServer`'s public key while the position log is symmetrically encrypted with a random key. The transaction number is left as plaintext. The symmetric keys are stored internally in the `vehicle` and given only on request to the `chargingAuthority` and even then encrypted with its public key. Thus there will be no legible information for eavesdroppers (see section 2.3).

A received `payment-Order` in the `commerceServer` causes a transaction transferring money from the vehicle owner's to the charging authority's account. When the payment is made, a receipt is sent to the `vehicle` and a `paymentConfirmation` is sent to the `chargingAuthority`. The receipt contains the `payment-Order` and information on when the payment was made. Note that the `commerceServer` is unable to read the time-position log since it does not have access to any keys. Nor can the `chargingAuthority` read it (should they gain access) before receiving the secret keys. The `paymentConfirmation` contains only the paid amount and the transaction-identity.

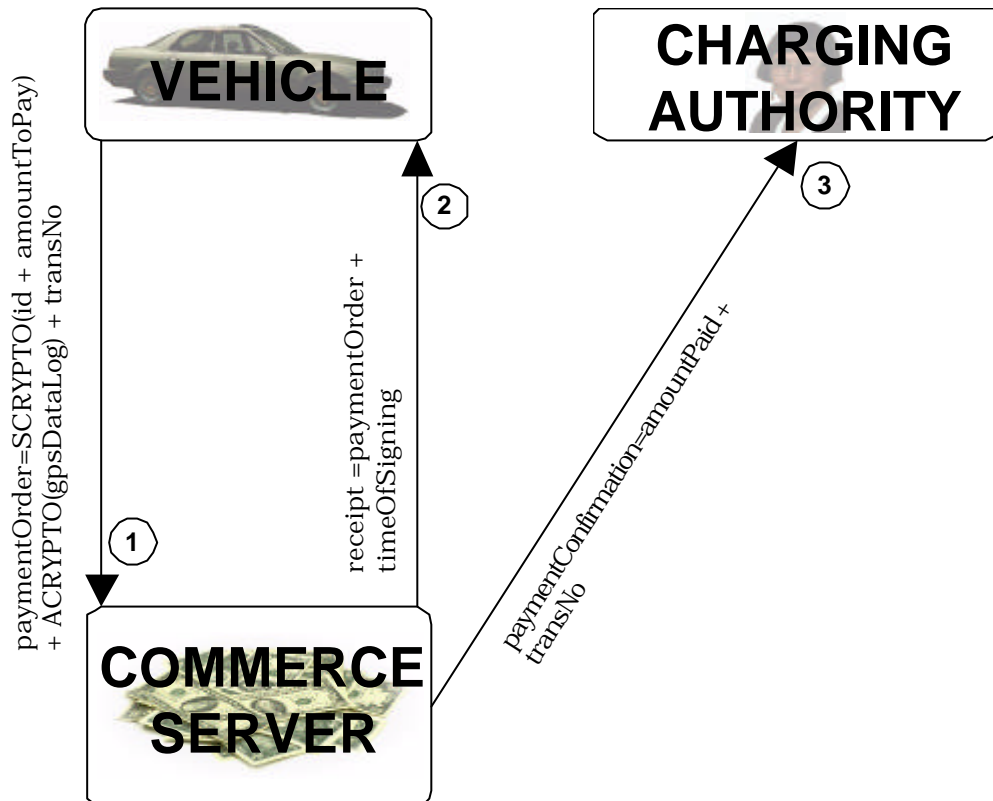


Figure 3. Information flow during the payment procedure

3.3.3 Compliance check procedure

The compliance check is initiated when the observer sends an observation to the chargingAuthority. This triggers a number of actions:

After a delay long enough to allow the vehicle to pay and get a receipt, a control-InfoRequest is sent from the chargingAuthority to the vehicle. The request specifies an observation number and which time interval that is to be controlled, this of course contains the time the observation was made. The vehicle then sends back a controllInfo-package containing the observation number, the relevant receipts and the secret keys are encrypted with the chargingAuthority's public key.

The first control-function is to check that the payment has been made before the request. If not, the vehicle could have "tailored" the information, sent to and signed by the commerce server, taking into account where and when the control took place. The position information in the receipt is then decrypted, compared with the observation and the amount that should have been paid is computed. Finally this is compared with what was actually paid. Any discrepancies are registered.

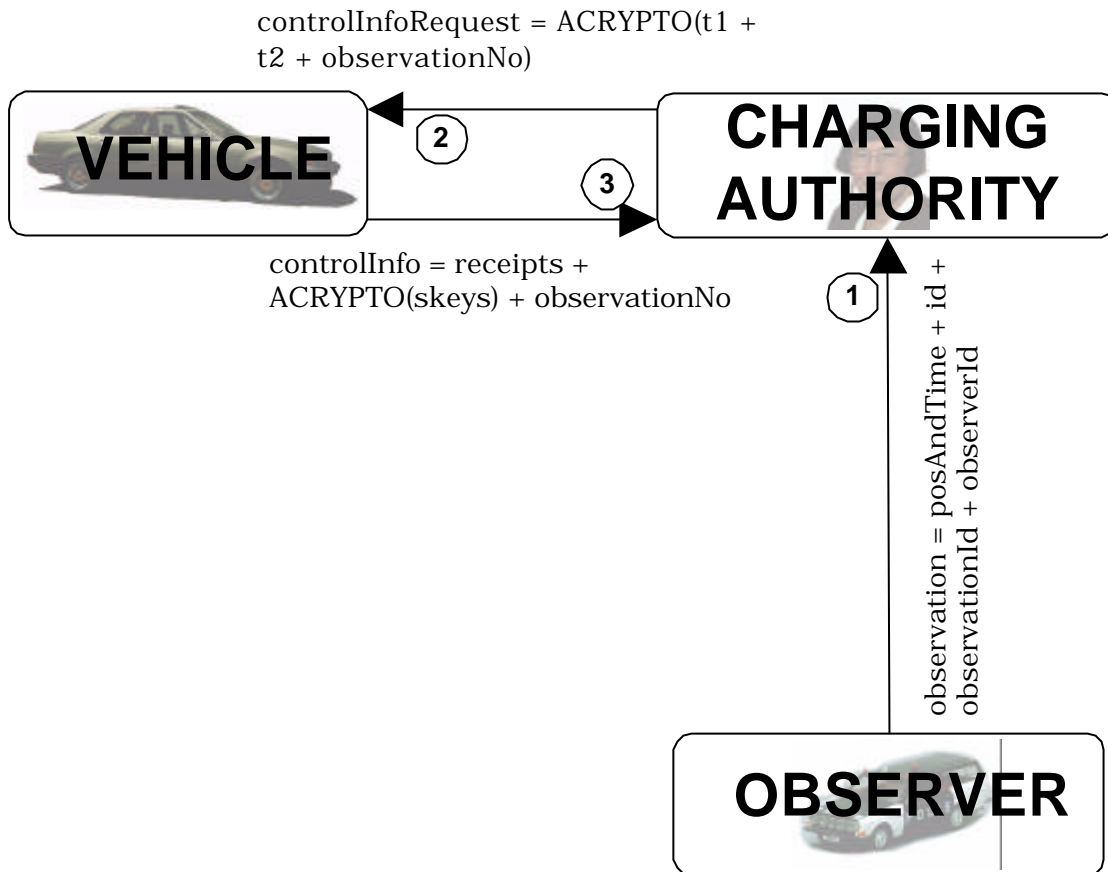


Figure 4. Information flow during the compliance check procedure

3.4 Components and objects of the vehicle

The vehicle is a sort of container for a number of sub-objects. Most of them have a direct correspondence in the physical part of α -BESTYR while others do not. I will use the word object and a special font for virtual parts to distinguish them from physical parts, which I will call components.

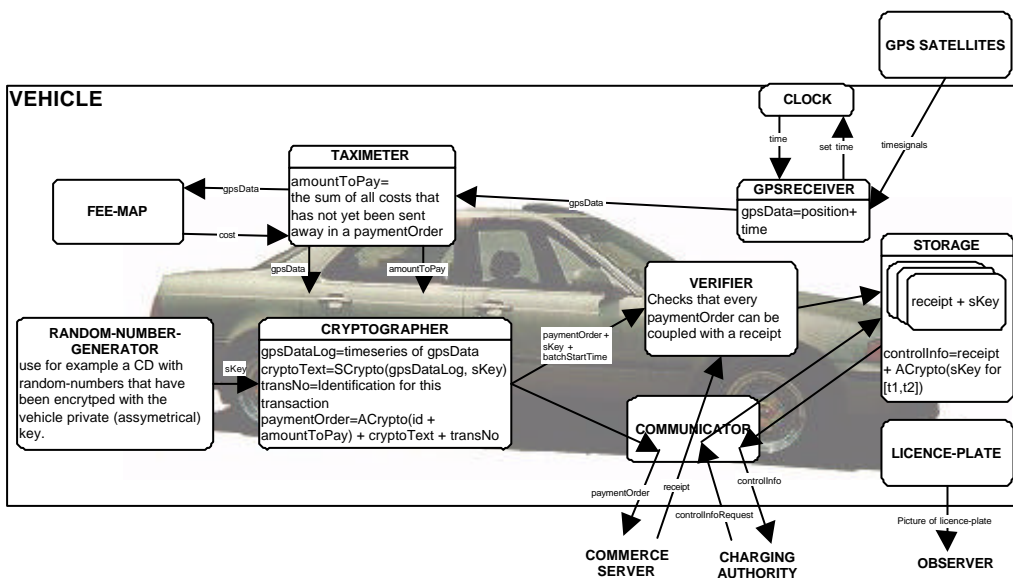


Figure 5. Informationflow between objects and components in the vehicle

3.4.1 gpsReceiver and clock

This code-object receives input from the physical GPS-receiver with information expressed according to the NMEA-protocol (see Appendix). It then applies two filters, first one that only lets messages of type Global Positioning System Fix Data (GGA) through. These messages carry information about the longitude, latitude, geoidal height and time of day. α -BESTYR does not use the time information but instead relies totally on the internal clock. A second filter is used to ward off reflected signals (i.e. from high buildings in urban areas). It uses three space-time points to estimate the acceleration. If the absolute value of the acceleration is greater than 4 m/s^2 the third point is deemed implausible and is thrown away. In coming versions of BESTYR, time and week-number should be read from the GPS-satellite.

3.4.2 taximeter and feeMap

The `taximeter` calculates the amount to pay using input from the `gpsReceiver` and the `feeMap`. It reads data from the `gpsReceiver` in pairs. By means of interpolation it extracts points that lie no more than ten meters apart. This interval should be sufficient to approximate the cost integral described in section 1.1 with a sum. The interpolated points are then the counterparts of position \bar{p} and the `feeMap` the counterpart of the cost-function f . The cost is accumulated in the taximeter in two variables, one that works as a kind of trip-meter showing the amount the driver has used so far, and a temporary variable read by the `cryptographer`-object and then reset.

3.4.3 cryptographer

The `cryptographer` is the heart of the code reading, assembling, encrypting and putting on queue for sending in the `communicator` and verification in the `verifier`. It reads space-time points (`gpsData`) from the `taximeter`. When the batch is large enough the `cryptographer` puts them in a package that is symmetrically encrypted with a random key. Then the cost for the movements described in the batch is read from the `taximeter` and put in a `payment-OrderPart`-package along with the vehicle registration number and are encrypted with the `commerceServer`'s public key. Two copies of a `payment-Order` object are now assembled consisting of the encrypted batch, the `paymentOrderPart` and a random transaction number in plaintext. One copy is sent to the `commerceServer` and the second copy is sent to the `verifier` along with the secret key used (`sKey`) and the time at which the measurements in the batch started (`batchStartTime`).

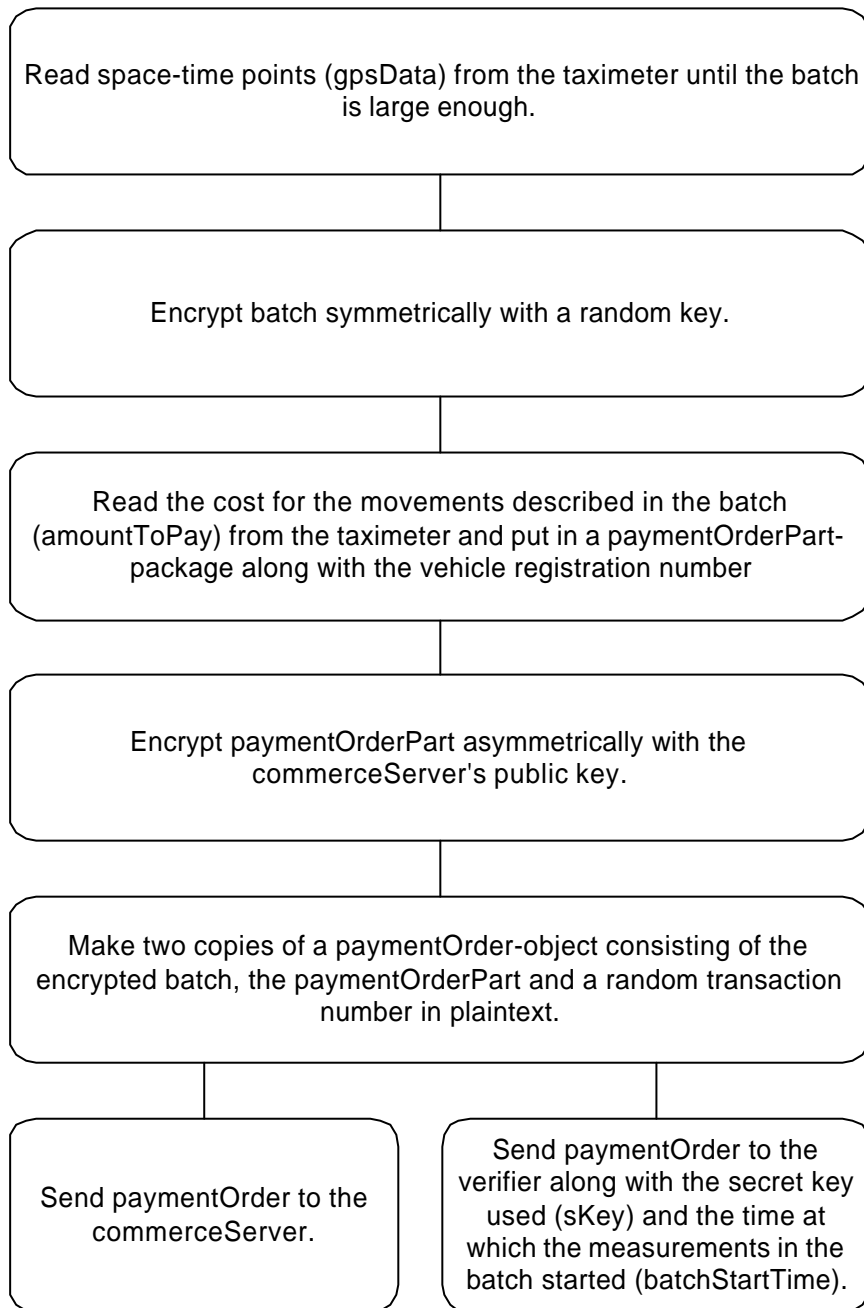


Figure 6. cryptographer task-diagram

There are at least three reasons for sending space-time points in a batch as opposed to encrypting and sending them one by one:

1. The most important reason is perhaps that it is a way to reduce the cost of sending data. The cost will probably be based on message size and possibly on the number of connections that have been made. In a batch there is only one header for the encryption algorithm instead of one for every space-time point. Of course you only have to make one connection if a batch is used rather than many if you sent each of them one at a time.

2. The encryption of the space-time points is easier to break if the packages are small since the redundant data (in the form of headers) is relatively larger.
3. Even if some attacker with access to the `commerceServer`'s private key (perhaps a malicious employee) not is able to read the encoded space-time batches he/she could still, by comparing with data from a `feeMap`-object (those would have to be publicly available) deduce how the vehicle has moved. The information needed would then be a starting position and the `amountToPay` for sufficiently small intervals. The risk for this kind of route deduction is almost totally eliminated by making the intervals big.

How large then is the “large enough” batch referred to above? I think that sending one every fourth hour could be suitable. It would save space but still have quite a short time interval, which means that compliance check could be carried out within reasonable time. If space-time-points are logged at the rate of one every other second one then one batch contains 7200 elements. However this can probably be significantly reduced by “smart logging” outlined in chapter 9.

3.4.4 Random-number-generator

Generating random numbers may seem like a trivial thing but it is not, as anyone who knows a little about cryptography is well aware of. α -BESTYR uses the Java key generator function `javax.crypto.KeyGenerator` for symmetric keys and `java.security.KeyPairGenerator` for asymmetric keys. In a real system it would be very unwise to trust that the keys generated by these Java packages are random enough, but α -BESTYR is only a demonstration.

So how does one go about generating random numbers?¹⁷ The best way is to observe some process in the physical world, where randomness is abundant, and somehow extract a number from it. The classic example is to make two measurements of the time-interval between two gamma rays from a radioactive source. If the first measurement is greater than or equal to the second then the output is one, otherwise it is zero. Thus one random bit has been generated. In similar ways one could imagine using air-turbulence or maybe the least significant bit of the angle of the steering wheel. My personal (not very realistic) favourite is to use a lava-lamp (see <http://lavarand.sgi.com/>).

Other possible approaches are to use so called pseudo-random functions or a CD of random numbers provided by some independent party and encrypted with the vehicle's private key before usage. A great advantage is that the rate at which random-numbers are to be created can be slow, only one every fourth hour is needed. A lot more can be said on this subject, but for now I will be content with the conviction that sufficiently random numbers can be obtained at a sufficient rate.

3.4.5 verifier and storage

The verifier checks so that a `receipt` eventually confirms that each `paymentOrder` has been carried out. One of the system requirements is that only the protocols and algorithms have to be trusted, not the other actors of the system. To achieve this the `vehicle` has to check on the `commerceServer` all the time to see that it follows the protocol. When the `payment-Order`, the `sKey` and the `batchStartTime` are received they are put in a queue in the `verifier`. Whenever a receipt from the `commerceServer` comes in, granting a successfully done payment, it is

put in another queue. Both queues are then checked for matching elements. If found, they are removed from the queues and a `receipt` along with the `sKey`, is sent to the `storage`, indexed with the `batchStartTime`.

The `storage` is called on when the `chargingAuthority` performs a compliance check. A `controllInfoRequest` is then sent to the vehicle's `communicator` and redirected to `storage` that replies by sending a `controllInfo` object to the `chargingAuthority`. This object contains `receipts` and `keys` for the time-interval $[t1, t2]$ specified in the `controllInfoRequest`.

3.4.6 communicator

The `communicator` is a generic object used in all four actors. All information sent to and from the actor passes through it. The final destination of incoming information is determined by an `inRouter` on the basis of what type of message it is. A `receipt` is sent to the `verifier`, a `controllInfoRequest` to the `storage` and so on. The hardware is in this case a GSM mobile phone that maintains a modem connection to Internet at all times. Of course this consumes an absolutely ridiculous amount of bandwidth. Dialling up every time a connection is needed could alleviate this problem. However, communicating with GPRS (see section 2.5) is even more bandwidth efficient and will be used in the next generation of BESTYR.

3.4.7 Licence plate

It is necessary for the compliance check procedure that the observer can identify vehicles. This is done by visual inspection of the licence-plate. This might seem like an insecure procedure, as the licence plate can be covered with mud, painted over, repainted to another number and so on. However, experiences from Oslo show that it works. And my guess is that identification will be done visually for a long time to come.

3.5 The commerce server

The object structure of the `commerceServer` is very limited and should not be interpreted as a proposal for how a commerce server should work. Instead it is the minimum needed to make the interaction between `vehicle` and `chargingAuthority` work in a realistic way. The rest of the financial infrastructure is completely omitted. I will assume that some kind of electronic financial system where one can order money to be transferred from one account to another will be available to later versions of BESTYR. If BESTYR is implemented, providing the commerce server will be a huge business opportunity. This should lead to a situation where many financial institutions will compete for customers, that is, the vehicle owners. This is a very desirable situation for financial reasons and also fulfils the requirement stated in section 1.2.1 because it allows the user to choose between different providers.

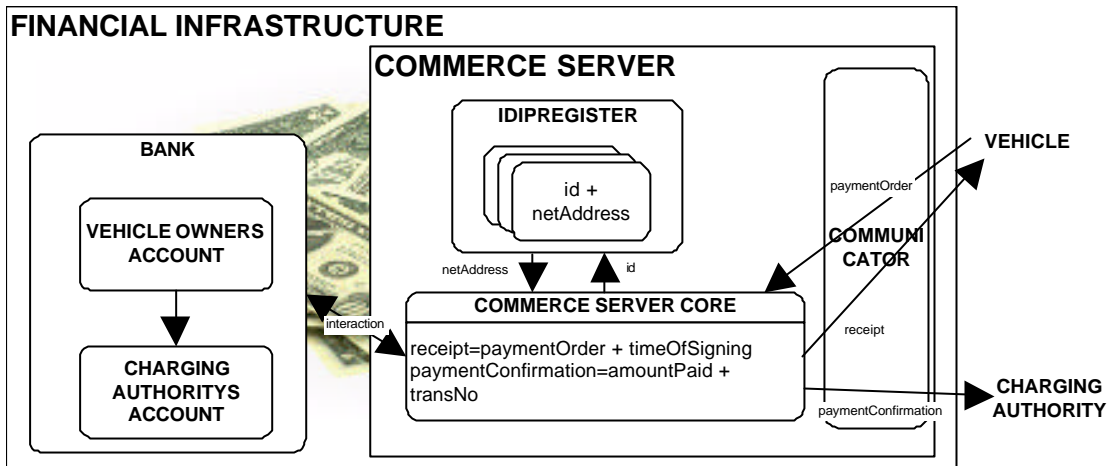


Figure 7. Informationflow between objects in the financial infrastructure

3.6 The observer

One can imagine two types of observer terminals; both are equipped with a clock and a GPS-receiver. The difference lies in how the identification is done. The simple unit is just a keyboard and the licence plate number is typed in after an observation made by a human. The more powerful unit has a video camera connected to OCR-software (Optical Character Recognition software) that can read the licence plate. Such a unit can for example be placed over busy roads to check every twentieth or thirtieth car.

The observation of a vehicle is sent back to the chargingAuthority over a secure channel or encrypted with a secret key. This part of the key-management is trivial. As with the commerce server the implementation in α -BESTYR is purely for demonstration. Instead of an input terminal or a camera, a dialog is shown, asking if you want to simulate observation of a cheater or of a non-cheater.

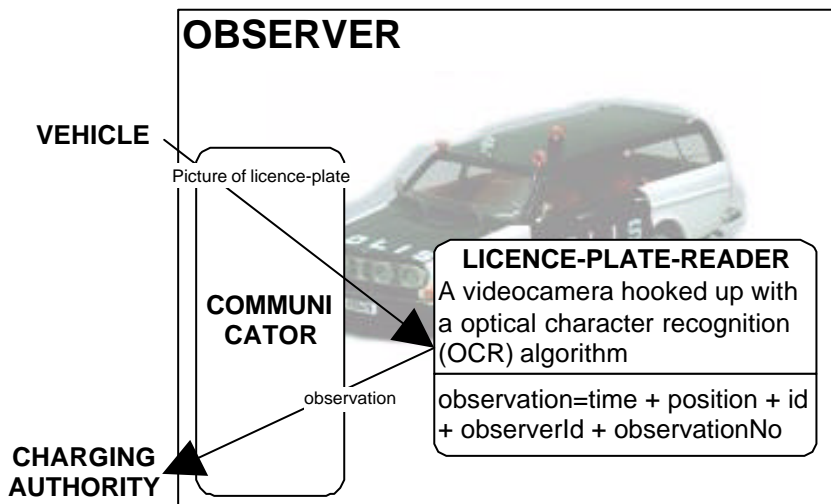


Figure 8. Informationflow between objects in the observer

3.7 Components and objects of the charging authority

The charging authority consists almost completely of software and should, unlike the `commerceServer` and the `observer`, be seen as my idea of the final version.

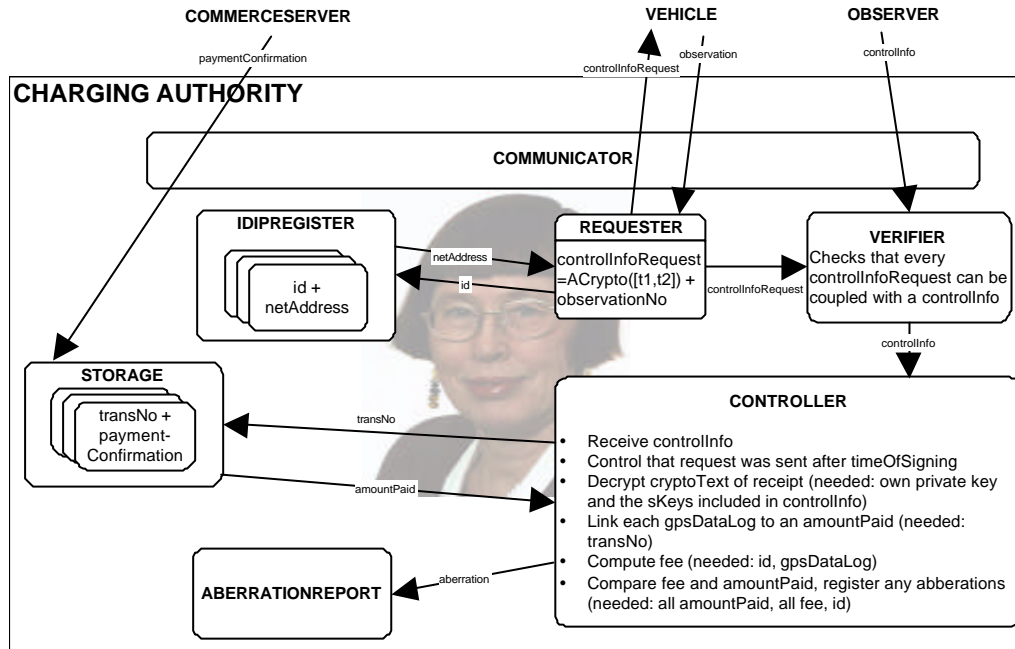


Figure 9. Informationflow between objects in the charging authority

3.7.1 communicator and storage

The same generic communicator object as in the other three actors is used. The `inRouter` can receive `paymentConfirmation`, `observation` and `controllInfo`. The `paymentConfirmation` is sent directly to `storage` and indexed by its `transNo`.

3.7.2 requester and idipRegister

When an `observation` arrives it is sent to the `requester` whose only task is to get the address of the vehicle that was observed from the `idipRegister`, and send a `controllInfoRequest`. But, as mentioned earlier, there must be a certain time lag between the `observation` and the `controllInfoRequest` so that there is no “tailoring”. The delay is set by the `OB-SCONTRDELAY` constant. The length of the time interval for which one asks for control information is set by the `TIMEINTERVCONTR` constant. A copy of the `controllInfoRequest` is sent to the `verifier`

3.7.3 verifier, controller and aberrationReport

The `verifier` makes sure that every request actually gets an answer. When a `controllInfo`-package comes in that can be coupled with a `controllInfoRequest` they are both sent to the `controller` where the procedure is described under section 3.3.3. Any discrepancies are sent to `aberrationReport`. In α -BESTYR that only means printing it out on the screen.

4 Compliance check

4.1 Observers

As I have mentioned earlier, collecting data for the compliance check procedure can be done in a number of ways. One can differentiate between mobile and stationary observers. The mobile observers perform a function that is analogous to the traffic control we have today. When the police stands at the roadside with a speedometer to make sure people do not exceed the allowed speed limit they might just as well also make an **observation** that at a later time enables the **chargingAuthority** to ask the **vehicle** to send its **receipts** for that particular time. When traffic wardens are out to control people's parking they could just as well make **observations** and send **observations** to the **chargingAuthority**. It is cost efficient and easy to do this, although this might be too easy as some argue (this is further discussed in chapter 6).

Stationary observers are essentially the same kind of stations that are used in the Oslo model. Video cameras are mounted for road surveillance at the major entrances to a city. There are some interesting variations on this theme however. It is desirable to reduce the number of cameras since a camera coupled with a good OCR algorithm is expensive. To continuously have cameras at all entrances might also allow for more control than is really necessary. But if for example only half of the entrances are controlled with cameras that are moved around, the cheaters will quickly adjust and use the routes that are not surveyed. A solution to this is to let some fraction of the cameras be real and the rest be false. The positions of the false and the real cameras can then be shifted around every once in a while.

There are many complicated ways of trying to foil a charging system such as BESTYR but one must not forget the most obvious one. Someone might just rip out anything that has anything to do with a charging system from the vehicle, which would render it mute as well as blind. If the licence plate is an electronic one then the vehicle will also have become invisible to the system. This is the most important reason for having an observer and why we need to detect the vehicles themselves, not some electronic badge or smartcard. Such devices can be used to pay but not for identification.

4.2 Time delay

After an observation the **chargingAuthority** waits the **OBSCONTRDELAY** before it sends out its **controlInfoRequest**. The delay can be of any length as long as the request is received before the receipts are thrown away. I will call the time that the receipts have to be saved the control period. It should be set rather generously to accommodate for various delays that could occur. My suggestion is 72 hours.

4.3 Checkpoints

It is fortunate that urban areas where the distance fee will be high are also the areas where checkpoints are easy to set up. In rural areas setting up a checkpoint is expensive compared to the fees collected but since fees are low or zero they are not really needed anyway.

The geographical location of a checkpoint strives to ensure good surveillance effect while preserving fairness. One consequence is that performing compliance checks inside a tunnel or some other place where there is no possibility for the GPS-device receiving a signal is a bad idea. BESTYR interpolates between logged space-time points and can in that way sometimes make up for bad GPS-reception. When interpolation is insufficient the checkpoint has to be moved.

4.4 Who pays?

What then will happen when a vehicle is found to not be in compliance with the BESTYR system? Who is legally responsible? Earlier I have, without motivating, stated that such responsibilities falls on the vehicle *owner*. This is by no means self-evident. However it is a convenient solution both from a legal and technical point of view. In “Breaking the Logjam”¹⁸, a white paper from Great Britain the following is said on the subject:

The Government intends that the registered *keeper* of a vehicle should be responsible for paying any penalty charge notice (PCN) following non-payment of a road user charge. (There would of course be a defence where a vehicle had been taken without the owner’s consent.) *Driver* liability would require the enforcement body to be able to identify the person driving the vehicle at the time that a charge was not paid. That would either require camera evidence of failure to pay a charge to include a photograph of the driver’s face, which raises serious concerns about privacy, or a lengthy and bureaucratic process of swearing statements and attempting to transfer liability.

Who then is responsible to pay the road fees? The BESTYR system has to judge from whom is registered to own the SIM-card in the vehicle. This introduces the possibility of having personal SIM-cards where there are many users of one vehicle, for example in families, companies and car-pools.

5 Security

5.1 A virtual control zone

Why, could one ask, does α -BESTYR send `controlInfoRequests` that specifies a time *interval* rather than a point in time that is to be controlled. There are two reasons for this. The first is a simple safeguard against unsynchronised clocks. That the clock in the `vehicle` is off by a minute or two compared to the clock in the `observer` should not result in the `controlInfo` not containing the correct co-ordinates.

But this does not account for the random positioning of the actual observation in the control time interval, which instead has been used to create a virtual control zone. (Actually in its current implementation, with no "time margins" two unsynchronised clocks and bad luck can still cause a vehicle to send back `controlInfo` that does not contain the controlled position, this will change in future versions.) The virtual control zone exists since it is impossible for a `vehicle` to deduce exactly when it was controlled by just examining the `controlInfoRequest`. In this way the `chargingAuthority` can have an extra protection against information tailoring schemes that somehow take advantage of knowing exactly when control took place. If this feature is actually helpful or only obscures the ideas of BESTYR still remains to be thoroughly examined.

5.2 Algorithms and key lengths used

As is already mentioned in the problem description α -BESTYR is not the final product but a first draft. To analyse algorithms for encryption is a difficult task and well beyond the scope of this master thesis. Therefore rather arbitrarily the symmetric algorithm RC4 (stands for Rivest's Cipher 4 although some claim it should be interpreted as Ron's Code 4) and the asymmetric algorithm RSA (initials of the authors surnames) have been chosen. Key lengths have been set to 128 respectively 2048 bits based on the conservative recommendations in Schneier's "Applied Cryptography"¹⁹. RC4 is a variable-key-size stream cipher developed in 1987 by Ron Rivest. The source code became public in September 1994. RC4 is used in many commercial cryptography products, for example Lotus Notes and Oracle's Secure SQL. A trio, the same Ron Rivest that wrote RC4, Adi Shamir and Leonard Adleman, wrote RSA. It was the first code to implement the public key ideas from Diffie and Hellman's "New Directions in Cryptography". The French banking community and the Australian banking community have both standardised on RSA for public key encryption.

5.3 Cryptographic attacks

The core of α -BESTYR is the payment and the compliance check procedure. These procedures are dictated by communication protocols that are built on cryptographic techniques such as ciphers and signatures. If these building blocks can be broken then obviously the whole protocol falls to pieces.

5.3.1 Exhaustive search

If a person tries to figure out the secret or private keys for a cipher or a signature with access to the algorithm used, the ciphertext and some knowledge about the plaintext is called a known-plaintext attack. For example in the case of trying to decrypt the encrypted time position log one would know that the result should describe a continuous trace, perhaps one even knows that the starting point is the vehicle owner's garage. Another common method is to look for a standard header. The most obvious way of launching a known-plaintext attack is to perform an exhaustive search of all keys. That is, try to decrypt the ciphertext with one key after another until the information one gets matches the plaintext.

5.3.2 Physical attacks

A completely different method is rubber-hose cryptanalysis or its close relative the purchase key attack. As the names imply the keys are in these cases found through threat, blackmail or bribery. Remember that keys are in our case not memorised passwords but SIM-cards and long sequences of numbers written to some kind of digital media. Another variation on this theme is to break in and steal the key or the desired information directly. It is also possible that a wrongdoer changes the equipment in the vehicle to gain information or simply with the intent to "frame" the vehicle owner.

5.3.3 Passive attacks

The attacks on the protocol can be grouped into passive and active. Passive attacks basically means eavesdropping. Then one can try to decipher the captured cryptotext or simply perform traffic analysis to gain information from the length of the message or the time it was sent. How is α -BESTYR vulnerable to this? Deciphering is at least in the foreseeable future next to impossible to perform because of the combination of good algorithms and long keys. Traffic analysis will give away some information but not much. I will discuss this further in chapter 6.

5.3.4 Active attacks

When an unauthorised actor takes part in a communication protocol it is called an active attack. I will mention some of these variants here.

Masquerade is when an attacker tricks the legitimate actors into performing the communication protocol with her/him rather than the intended counterpart. The man in the middle attack is a double masquerade where the attacker captures all communication between the legitimate parties, alters it to suit her/his needs and then lets the message reach its intended destination.

α -BESTYR is very sensitive to this kind of attack due to its initialisation procedure where the public keys are exchanged. An attacker that intercepts all public keys and substitutes them with her/his own can then effectively control all communication. To reduce the risk of this the keys should not be shared on start-up before each trip but more seldom then very strict security measures are feasible. One could imagine that the sharing of keys takes place at the same time as the *feeMap* is updated at some kind of yearly vehicle inspection (in Sweden "bilbesiktningen", in the United Kingdom "MOT").

A replay attack is when a previously captured message is resent at a later time. An attacker would in this way be able to make unauthorised money transfers from the vehicle owner's to the government's account. There is no financial gain for the attacker but the motive could simply be to cause trouble. α -BESTYR is vulnerable to this kind of attack. The fix is to use so-called nonces. When an actor initiates a contact the response is to return the transaction number or observation number together with a random number which is the nonce. When the initiating actor receives this he/she encrypts the nonce with his/her private key and sends all of it back so that the random number can be decrypted to verify that it is the same number. Since the random number is (for practical reasons) always different this makes every conversation unique. The transaction number and the observation number are sent along as references.

Another effective attack that can be performed by the vehicle to avoid payment is denial of services. When the chargingAuthority sends a controlInfo the vehicle can simply refrain from answering saying that the communication equipment was broken at the time. The simplest solution would be to legally require that the vehicle keep its equipment functioning. The charging authority can provide test-protocols with a recommendation to run them say every week.

5.4 Does α -BESTYR fulfil the security requirements?

The former section is summed up in the comments below on all the items that were listed as security requirements in section 1.2.2. In α -BESTYR neither automatic signing of all messages nor counter-measures against the man in the middle attack have been taken but in the list below I will disregard these two weaknesses since they are well understood and will corrected in coming versions.

Requirement	Fulfilment
Segment integrity	α -BESTYR contains no "black boxes" that the proprietor can not alter. Every actor has the full right to make changes in her/his own physical system as long as the communications that are required still can be performed. However, a malicious actor could break into the vehicle to tamper with its equipment and thereby compromise segment integrity.
Message integrity	Unauthorised entities can not change message contents without being noticed because of the signing.
Entity authentication	The correctness of the entity identity rests on management of the asymmetric keys being safe.
Message authentication	The correctness of the origin is proven through signing.
Message timeliness	No timestamps are needed in α -BESTYR. The replay attack is warded off with the use of nonces.

Non-repudiation	Both the payment and the compliance check procedure employ a verifier (in the vehicle and the charging Authority respectively) to see to it that a response confirms delivery, submission and receipt of messages.
Accountability & audit	The actors' responsibility for their own actions so that violations of system security may be traced uniquely to them is a legal matter.
Confidentiality	That message contents are not disclosed to unauthorised entities rests on good protection against rubber-hose attacks, purchase key attacks and break-ins.
The user should be able to convince himself/herself of the legitimacy of collection and charging equipment and operators.	This is achieved through signing of all messages.
The user should be able to convince himself/herself (and others) that balances cq. Service rights are properly set/increased/decreased.	This is achieved through trust in the commerce server in much the same way one trusts ones credit card operator.
System malfunctioning not due to her/his own handling should have no financial consequences for her/him personally.	This is a legal matter.

6 Personal integrity

On the wall were the police ear and the police eye, as effective in darkness as in light. No one could find them anything else than well motivated: what hearths for espionage and conspiracy could not the parental rooms otherwise become, ...²⁰

Above is an excerpt (my translation) from Swedish writer Karin Boyes dystopic novel *Kalloscain*. It describes the fear of surveillance from governmental organisations and illustrates one extreme of the sentiments that have been expressed in response to the road-pricing idea. α -BESTYR will not peek into people's bedrooms to ensure compliance but will function similar to ordinary traffic inspection much like speed limit controls today. So does a threat to personal integrity exist at all? Do we have to worry? I believe so. We have to be very clear about what risks we are introducing. Two facts are important to hold in mind. Firstly, a control procedure that is performed only on a small scale is something qualitatively different from when it is performed on a massive scale. Secondly, everyone might not at all times find the government completely trustworthy. These people will not be satisfied with giving a governmental organisation power to perform extensive surveillance. Not even if the use of this power is heavily restricted in law because why should an untrustworthy government follow the law?

6.1 Cameras

A road-pricing system of the sort that I have proposed certainly requires extended control, primarily through video cameras in the stationary observation units. Of course only the registration number not the picture of the vehicle will be saved but given the second argument above, one still has to be very cautious. The first argument also applies, road-pricing control is something qualitatively different from speed limit control because of the frequency with which it is performed. The question is: can the increased control of the citizens be motivated by the good that can be done by the system which it supports?

The Swedish political investigation "Miljöstyrande vägavgifter i tätort"²¹ looks into the legal consequences of a road-pricing system. There it is stated that guarding personal integrity is an old and strong tradition in Swedish law. They also establish that some kind of surveillance is necessary to guarantee compliance with a road-pricing system and that using video-cameras is the only feasible solution in practice.

The investigation then goes on to say that Swedish law allows camera surveillance used in a road-pricing system and concludes (my translation):

The report establishes that it is not certain that the payment can be performed anonymously. In spite of this, the charging system as such can not be considered a major trespass on personal integrity and the control functions that the system requires are within the boundaries of what can be accepted to lower the negative impacts of road traffic on the environment. Road-pricing to lower environmental impact is acceptable from a protection of personal integrity standpoint, according to the report.

6.2 Receipts

Obviously when a `controlInfoRequest` is received the vehicle has to send a `controlInfo` package or be fined. Inside the receipts are time-position logs and the charging authority will have access to the necessary keys to read them. Thus more information than just a confirmation of what the charging authority already knows will be available. The receipts put the information in batches and can only be retrieved as such. In a worst case scenario the charging authority observes the vehicle just before or after a `paymentOrder` is sent. If the `controlInfoRequest` asks for ten minutes worth of receipts the vehicle might have to send him eight hours (two receipts) of it. The reason is that the virtual control zone in this case overlaps two receipts. The best way to remedy this problem is to see to it that although the `paymentOrder` is sent in one big batch it is encrypted in many smaller ones. This will enable the `commerceServer` to sign smaller batches of data and thus making receipts that only cover a shorter time interval, say ten minutes. This will be included in future versions of BESTYR.

6.3 Monitoring of the cellular phone radio-frequencies

Most of the information in the α -BESTYR system is sent via cellular phone to base stations via radio waves. It is not trivial to eavesdrop on such a conversation because of the jumping from frequency to frequency that is performed to avoid dropouts in the calls and to increase security. However, eavesdropping can be done. But all information is heavily encrypted and next to impossible to read without the key. Still traffic analysis, examining the length of the messages and when they were sent, can be performed. In α -BESTYR the length of the messages is unlikely to reveal anything but if this is a concern it is a simple matter to allow for padding of the messages with random numbers to make the lengths uniform. Nor is it probable that the time when the message is sent will reveal any information but if this is a concern no procedure is really time critical and so random delays can be introduced to completely obscure what time related information there was.

6.4 Base station triangulation

A well known, but by the general public, little discussed fact is that having a cellular phone switched on enables the phone operator to tell its position. The process is called base station triangulation. As of yet there is no regulations concerning this and so the information needed to perform base station triangulation is routinely logged and saved. The situation is not altogether unreasonable for personal cellular phones where the usage after all is a personal choice. But it would be unwise for a road-pricing to allow that kind of information spill. Fortunately, one can arrange it so that the phone in the vehicle is only switched on to send `paymentOrders` to the commerce server and look for `controlInfoRequests` and can be switched off in between. Any messages (`controlInfoRequests`) coming in while the phone is off are put on queue and downloaded when a connection for sending is established. This results in the phone operator knowing the vehicles position only for a short time during transmission and download, say once every four hours. Maybe there should be a possibility for the really cautious user that still wants to use the BESTYR to have all communications made via physical mail.

7 Paying outside a-BESTYR

Just because a road-pricing system is introduced, it does not mean that everyone will want to use an advanced technical solution. This sentiment is also expressed in the requirements of "Miljöstyrande vägavgifter i tätort". Alternative ways must be made available.

7.1 Advance payments

A rudimentary system uses advance payments. When the vehicle is observed it is the information is sent to the advance payments database. As long as *someone* has paid to give the vehicle permission to be in the given time and place all is good and well. Or the compliance check could be to actually stop the vehicle and ask for its ticket. In Sweden one could imagine taking advantage of the wide spread "ATG/Biljett direkt"-system for purchase of permission-tickets.

7.2 GSM positioning

A slightly more technically advanced system would be to use the SIM-card of a cellular phone for identification at a central server that takes care of all computing and billing. Positioning is achieved through base station triangulation. The infringements in personal integrity due to continuous tracking of the vehicle can be considered acceptable since other alternatives are available. This service could be very attractive to temporary visitors from abroad.

8 Conclusion

In this report I have briefly covered many of the problems and considerations that have to be taken into account when designing a road-pricing system. Such a general approach is motivated by the aim to provide a starting point for further discussion around a technical system for road-pricing. The process of programming the demonstration system have clarified the ideas and helped in writing the report.

The fee, F , is computed and paid with the help of four communicating actors. Each actor, the **vehicle**, the **commerceServer**, the **chargingAuthority** and the **observer**, is implemented in a separate Java application that can reside at a separate IP-address. The **vehicle**-unit must be mobile and is therefore powered by a portable computer communicating through a cellular phone. Furthermore it has to be able to determine its geographical location and uses a GPS-receiver for this.

α -BESTYR has three different communication procedures. Initialisation is when the **vehicle** reports its dynamically allocated IP-address and also when the sharing of public keys take place. The current implementation will change with the introduction of GPRS-communication, which provides static addressing. The sharing of keys will also be changed to only take place at safe communication stations in order to avoid a man-in-the-middle attack.

Payment is the most central procedure. That it is performed correctly is ensured through spot checks according to the compliance check procedure. Together payment and compliance check forms an adjudicated communication protocol guarding both security and integrity.

Observers that provides the data to perform a compliance check can be both stationary and mobile, where is more effective with respect to quantity while the second is more unpredictable in its positioning and thus provides observations of a higher quality. Factors such as the possibility for the vehicle to make a correct measurement of its position and the time-interval at which payments are made also have to be taken into account when performing compliance checks. A number of attacks against the system and their counter-measures have been discussed.

The concern that a road-pricing system will result in severe infringements on personal integrity has been discussed. It is established that infringements can be considered minor compared to the benefits of such a system.

The report and the demonstration system have not found any problems or weaknesses that makes α -BESTYR impossible to implement.

9 Further work

Message queue for vehicle: In order to enable the vehicle to have its cellular phone mostly switched off a message queue service has to be implemented. This introduces the communication middleman as a fifth actor with the task to provide a server that takes care of the vehicles incoming communication.

Smart logging: Find a way of describing an arbitrary space-time log that minimises its size. The precision in the information should not be higher than is needed to compute a correct fee.

Smaller receipts: To let receipts describe a shorter time interval increases personal integrity (see section 6.2) but weakens its cryptographic strength (see section 3.4.3). Find an ideal trade off between the two.

Virtual Control Zone: Examine the benefit of not letting the vehicle know exactly when it is controlled as described in section 5.1.

Collection of parking fees: An implementation of BESTYR with some slight extensions allows for collection of parking fees. Look into what changes that have to be made to the charging model (the computation of F) and requirements on when payments are to be made.

Value-adding services: User acceptance can probably be greatly enhanced by adding services such as digital road maps, traffic information and so on. The vehicle has access to a wealth of data (that is not available to anyone else). Nothing prevents that information valuable to the driver is distilled and presented on a screen.

Formal analysis of authentication and key exchange protocols: Use BAN logic and tools such as the NRL Protocol Analyzer²² to determine if the communication protocols in α -BESTYR are waterproof.

Virtual Private Networks (VPNs): Evaluate if it would be beneficial to substitute some or all of the cryptographic functions in α -BESTYR with a VPN.

Study user interface: Make a detailed study of the visual and aural user interface with special attention paid to traffic safety. A good place to start would be the report “HMI knyttet till yrkessjåfører” written by Hans Myrhaug at Stiftelsen for Industriell och Teknologisk Forskning ved NTH (SINTEF) in Norway.

Technical review: Decide on what technical components that are to be used.

10 List of abbreviations

BESTYR	Betalning av miljöstyrande avgifter för bilar (Payment of Environmental Fees for Cars)
DSRC	Dedicated Short Range Communications
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for mobile Communications
ISP	Internet Service Provider
NMEA	National Marine Electronic Association
OCR	Optical Character Recognition
PROGRESS	Pricing Road Use for Greater Responsibility, Efficiency and Sustainability in Cities
SIM	Subscriber Identity Module
VPN	Virtual Private Network

11 Appendix

11.1 IP-addresses

An IP-address is the identifier for a computer or a device on a TCP/IP network and can thus be used for example to specify a message's destination address.

For example all URLs (not including library and file specifications) on the World Wide Web corresponds to an IP-address. These do not change very often and are therefore called statically allocated.

A computer connecting to Internet via modem has to go through an Internet service provider (ISP). The service provider does not have a specific IP-address reserved for every computer that it provides for. Instead the connecting computer gets assigned an address temporarily from a pool that the ISP has control over when it makes a connection. The IP-address is returned when the computer logs off. This is called a dynamically allocated IP-address.

When an IP-address is dynamically allocated only the ISP and the computer knows whom the address actually points to. Because of this the dynamically allocated party has to initiate any two-way communication protocol sending its own IP-address as the first message.

11.2 The NMEA-protcol

The National Marine Electronic Association (NMEA) standard 0183 is a protocol used by GPS receivers to transmit data. NMEA 0183 sentences are all ASCII. Each sentence begins with a dollar sign (\$) and ends with a carriage return linefeed (<CR><LF>). Data is comma delimited. All commas must be included as they act as markers. Following the \$ is the address field aacc. aa is the device id. GP is used to identify GPS data. ccc is the sentence name.

In α -BESTYR the only sentence that is read is Global Positioning System Fix Data (GGA) which among other things gives information on longitude, latitude and geoidal height.

12 References

-
- ¹ Uwe Albrecht, *Song of the ROBIN: GPS Drives Electronic Toll Collection Design*, GPS-World March 1995, Special Edition for Mannesmann Pilotenwicklungsgesellschaft mbH, Germany
- ² Wil J. Van Gils, *Why do we need Public Key Cryptographic Solutions in the form of "Slow and Fast Charge" in open Integrated Payment Systems for ADS?*, Commission of the European Communities, R&D Programme Telematics Systems in the Area of Transport (DRIVE-ATT), project ADEPT, March 16, 1993
- ³ Gert-Jan van Dijk (CMG), Feiko van der Veen (INTERCAI), Joop Gerritse (INTERCAI), *Stockholm Integrated Payment System*, STCS Requirements Specification, (STCS/SIPS-WG700), Preliminary draft, April 5, 1994
- ⁴ Wil J. Van Gils (Dutch Ministry of Transport and Public Works), Joop J. Gerritse (INTERCAI ATS) *Security: threat analysis and proposals for security algorithms*, Commission of the European Communities, R&D Programme Telematics Systems in the Area of Transport (DRIVE-ATT), project ADEPT, January 25, 1993
- ⁵ Wil J. Van Gils, *Why do we need Public Key Cryptographic Solutions in the form of "Slow and Fast Charge" in open Integrated Payment Systems for ADS?*, Commission of the European Communities, R&D Programme Telematics Systems in the Area of Transport (DRIVE-ATT), project ADEPT, March 16, 1993
- ⁶ Jonas Sundberg, *Preliminär projektplan för examensarbete vid KTH: BILENHETENS ER-LÄGGANDE AV AVGIFT SAMT KONTROLLFUNKTIONER INOM BESTYR-projektet*, September 1999
- ⁷ Kjell Larsson, *Så vill jag skapa en hållbar vägtrafik*, Dagens Nyheter, December 7, 1999
- ⁸ Ledare, *Bilavgifter på kollisionskurs*, Dagens Nyheter, December 13, 1999
- ⁹ Kjell-Olof Feldt, *"Oseriöst, Kjell Larsson!"*, Dagens Nyheter, December 20, 1999
- ¹⁰ Carl Cederschiöld, Sten Nordin, *Stockholm kommer aldrig att införa bilavgifter*, December 12, 1999
- ¹¹ Bruce Schneier, *Applied Cryptography*, second edition, sections 2.5 and 12.1, John Wiley & Sons, Inc. ISBN 0-471-11709-9
- ¹² *An investigation into the security issues surrounding data transmission and user anonymity using the Global System for Mobile Communication*, section 4.3.1, <http://www.alanta.demon.co.uk/GSMPaper/Title.html>, September 7, 1996
- ¹³ Bruce Schneier, *Applied Cryptography*, second edition, section 16.5, John Wiley & Sons, Inc. ISBN 0-471-11709-9
- ¹⁴ Niklas Laurell, Telia Mobile AutoCom, Conversation on the telephone February, 21, 2000
- ¹⁵ Johan Mellberg, Ericsson ERA, Conversation on the telephone, February 22, 2000
- ¹⁶ Bruce Schneier, *Applied Cryptography*, second edition, section 2.1, John Wiley & Sons, Inc. ISBN 0-471-11709-9
- ¹⁷ Bruce Schneier, *Applied Cryptography*, second edition, section 17.14, John Wiley & Sons, Inc. ISBN 0-471-11709-9

¹⁸ John Prescott, *Breaking the logjam*, section 3.33, Department of the Environment, Transport and the Regions, United Kingdom, December 14, 1998

¹⁹ Bruce Schneier, *Applied Cryptography*, second edition, sections 7.2 and 7.4, John Wiley & Sons, Inc. ISBN 0-471-11709-9

²⁰ Karin Boye, *Kalocain*, <http://www.lysator.liu.se/runeberg/kalocain>

²¹ *Miljöstyrande vägavgifter i tätort – ett förslag till lagstiftning*, Statens Offentliga Utredningar 1998:169, Kommunikationsdepartementet, Sweden

²² Bruce Schneier, *Applied Cryptography*, second edition, sections 3.4, John Wiley & Sons, Inc. ISBN 0-471-11709-9