



**NTNU – Trondheim**  
Norwegian University of  
Science and Technology

# Protocols for toll road systems

**Per Kristian J Fjellby**

Master of Science in Communication Technology

Submission date: June 2013

Supervisor: Danilo Gligoroski, ITEM

Co-supervisor: Tord Reistad, Statens Vegvesen

Norwegian University of Science and Technology  
Department of Telematics



**Title:** Protocols for toll road systems

**Student:** Per Kristian Jakobsen Fjellby

**Problem description:**

In a free-flow tolling system for cars, such as the AutoPASS system used in Norway, the cars do not have to slow down to pay the toll. The car is registered by reading equipment placed in the car or by an image of the license plate. If the car lacks such equipment and the license plates are not readable, identifying the car is almost impossible. The Office of the Auditor General of Norway (Riksrevisjonen) recently published a report showing that inadequate identification provides significant losses to the companies\*.

The thesis will examine current methods and protocols used for registering vehicles. Furthermore, this thesis will examine methods for better registration of vehicles through a theoretical simulation that models cars that pass through multiple toll plazas, and better methods for privacy. Enhancing privacy will come by first examining preserving technology and propose methods for increasing privacy within the boundaries of the current system.

**Responsible professor:** Danilo Gligoroski, ITEM

**Supervisor:** Tord Reistad, Statens Vegvesen

\* *Riksrevisjonens undersøkning av bompengeforvaltninga. Dokument 3:5 (2012/2013). See [32]*



## Abstract

A problem in a tolling system like AutoPASS is the number of unidentified passages due to unreadable license plates. As a consequence money is lost for the toll road companies. A scheme is proposed that uses anonymous statistics to aid in the process of allocating resources for manual controls. Due to legal requirements for anonymity of data produced at toll plazas, a model that simulates the traffic frequencies on Norwegian roads is developed and implemented in Java. Using the toll plazas that make up *Miljøpakken* in Trondheim as a starting point, a simulation generating three months worth of traffic amounting to almost 460 MiB of data is performed. The simulated data were checked for its reliability and similarity with real data. Calculations based on an optimistic estimate on the number of AutoPASS subscriptions with rebated fares have shown that nearly 370 000 NOK are lost due to unidentified vehicles over the three months simulated. The outlined solution shows that toll plazas with a higher number of unregistered passages can be identified and this information can be used in subsequent planning activities for the purpose of executing manual controls to reduce the losses.



## Sammendrag

Et problem i et bompengesystem slik som AutoPASS er antallet av uidentifiserbare passeringer som en følge av uleselige kjennemerker. Konsekvensen er at penger går tapt for bompengeselskapene. Et system er foreslått der anonym statistikk blir brukt for å allokere resurser til manuelle kontroller. På grunn av juridiske begrensninger på bruk av data som blir generert i bomstasjoner har det blitt utviklet og implementert en modell i Java som modellerer trafikk på veier i Norge. Ved å ta utgangspunkt i bomstasjonene som er en del av *Miljøpakken* i Trondheim blir det generert tre måneder med trafikkdata som utgjør nesten 460 MiB med data. De simulerte data blir sjekket både på pålitelighet og likhet mot ekte data. Kalkulasjoner basert på et optimistisk anslag av tallet på AutoPASS-avtaler med rabatterte passeringer viser at nesten 370 000 kroner går tapt på grunn av uidentifiserte kjøretøy i de tre simulerte månedene. Den skisserte løsningen viser at bomstasjonene med et høyere antall uregistrerte passeringer kan identifiseres og at denne informasjonen kan brukes i påfølgende planleggingsaktiviteter med formål om å utføre manuelle kontroller for å redusere tapene.

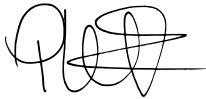




## Preface

This document is the result of a semester's worth of work related to AutoPASS and associated protocols. The document is submitted as part of the 5-year MSc program in Communication Technology at the Norwegian University of Science and Technology in Trondheim. I would like to extend my gratitude towards the supervisor and the professor, Tord Reistad at Statens Vegvesen and Danilo Gligoroski at the Department of Telematics, for their help and support.

Per Kristian Jakobsen Fjellby

A handwritten signature in black ink, consisting of a stylized 'P' followed by a series of loops and a horizontal stroke at the end.

Trondheim, June 2013



# Contents

<b>List of Figures</b>	<b>xi</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Algorithms</b>	<b>xv</b>
<b>Listings</b>	<b>xvii</b>
<b>Glossary</b>	<b>xix</b>
<b>Acronyms</b>	<b>xxi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Previous work . . . . .	1
1.2 Tolling in other countries . . . . .	2
1.3 Aim of this thesis . . . . .	2
1.4 Outline . . . . .	3
<b>2 Background</b>	<b>5</b>
2.1 AutoPASS in a nutshell . . . . .	5
2.2 Administrative outline of AutoPASS . . . . .	5
2.2.1 Actors . . . . .	5
2.2.2 Legal background . . . . .	7
2.3 Technical background . . . . .	8
2.3.1 Standards and directives . . . . .	8
2.3.2 AutoPASS system . . . . .	9
2.3.3 On-board unit . . . . .	9
2.3.4 Road side equipment . . . . .	10
2.3.5 Central System . . . . .	10
2.3.6 Interface on-board unit - charging point equipment . . . . .	11
2.3.7 Interface charging point equipment - central system . . . . .	14
2.3.8 Key hierarchy . . . . .	25

2.3.9	Key generation . . . . .	25
2.3.10	Message Authentication Code (MAC) generation . . . . .	28
<b>3</b>	<b>Methods</b>	<b>31</b>
3.1	Outline . . . . .	31
3.2	Statistics . . . . .	32
3.2.1	Scope of model . . . . .	36
3.3	Setup . . . . .	36
3.3.1	Computer hardware . . . . .	36
3.3.2	Installation . . . . .	37
3.3.3	mySQL setup . . . . .	38
3.3.4	Java . . . . .	38
<b>4</b>	<b>Results</b>	<b>41</b>
4.1	Simulation . . . . .	41
4.2	Program for displaying the statistics . . . . .	42
4.2.1	Database statistics . . . . .	42
4.2.2	Transactions per day-of-week . . . . .	43
4.2.3	Transactions per hour-of-day . . . . .	43
4.2.4	Unregistered transactions per day . . . . .	43
4.2.5	Unregistered transactions per toll plaza . . . . .	44
4.3	Evaluation of data . . . . .	44
4.3.1	Example of a specific case . . . . .	45
<b>5</b>	<b>Discussion</b>	<b>53</b>
5.1	Simulation . . . . .	53
5.1.1	Anonymization . . . . .	53
5.1.2	Executing a control . . . . .	54
5.1.3	Legal issues . . . . .	55
5.1.4	Related systems . . . . .	56
5.2	Anonymity . . . . .	57
5.2.1	Anonymity in AutoPASS . . . . .	57
5.2.2	How is anonymity handled in other countries . . . . .	60
5.2.3	A step toward bettering the anonymity in AutoPASS . . . . .	60
5.2.4	Evaluation of the protocol . . . . .	62
<b>6</b>	<b>Conclusion and further work</b>	<b>65</b>
6.1	Conclusion . . . . .	65
6.2	Further work . . . . .	66
	<b>References</b>	<b>67</b>
	<b>Appendices</b>	

<b>A Doppler shift calculation</b>	<b>71</b>
<b>B Data Encryption Standard (DES)</b>	<b>73</b>
B.1 DES with multiple keys . . . . .	74
B.1.1 2DES keying . . . . .	74
B.1.2 3DES keying . . . . .	75
B.2 Weak keys . . . . .	77
<b>C AutoPASS example contract (Fjellinjen)</b>	<b>79</b>
<b>D RSA and blind signatures</b>	<b>81</b>
D.1 RSA . . . . .	81
D.2 Blind signatures (With RSA) . . . . .	82



# List of Figures

2.1	Actors in the AutoPASS system . . . . .	6
2.2	Nodes in the AutoPASS system . . . . .	9
2.3	Norbit ITS FZ2358 OBU. The image is taken from datasheet [27]. . . . .	9
2.4	Figure of RSE near Sluppen bru in Trondheim . . . . .	10
2.5	Sequence diagram showing the messages exchanged between the on-board unit and the road-side unit. From [7]. . . . .	12
2.6	Block diagram of MAC generation . . . . .	30
3.1	24 hour traffic pattern . . . . .	34
3.2	Scaled weekly traffic patterns . . . . .	34
3.3	Reliability of AutoPASS charging . . . . .	35
3.4	Class diagram . . . . .	39
4.1	Graphics pane with graphing options . . . . .	42
4.2	Graphics pane with time fields . . . . .	42
4.3	Database statistics . . . . .	46
4.4	Day-of-week statistics . . . . .	47
4.5	Hour-of-day statistics . . . . .	48
4.6	Unregistered transactions shown per day of month . . . . .	49
4.7	Unregistered transactions shown per toll plaza . . . . .	50
4.8	Kroppan Bru 8 <sup>th</sup> February 2013 . . . . .	51
5.1	Toll plaza at Kroppan Bru, Trondheim . . . . .	55
5.2	Intersection between the <i>Motorist's</i> (M) used <i>ids</i> and the <i>Toll company's</i> (T) stored <i>ids</i> . . . . .	62
B.1	DES operations . . . . .	73
B.2	DES round structure . . . . .	75
C.1	Fjellinjen's AutoPASS user contract . . . . .	80





# List of Tables

2.1	Overview of the transaction file sent from charging point equipment to the central system. . . . .	15
2.2	Overview of the OBU status file parameters. . . . .	18
2.3	Parameters in a type 1 price record . . . . .	19
2.4	Parameters in a type 2 price record . . . . .	20
2.5	Parameters in a type 3 price record . . . . .	20
2.6	Parameters in a type 4 price record . . . . .	21
2.7	Parameters in a picture file . . . . .	22
2.8	Parameters in a currency file . . . . .	22
2.9	Parameters in an operator file . . . . .	23
2.10	Parameters in a blacklist file . . . . .	23
2.11	Parameters in an exception file . . . . .	24
2.12	Key hierarchy in AutoPASS. From [9] . . . . .	25
3.1	Toll plazas in <i>Miljøpakken</i> . Data from [25]. . . . .	32
3.2	Rates for the toll plazas in Miljøpakken. Values in NOK. From [11]. Columns with * are for vehicles weighing over 3.5 metric tonnes. . . . .	33
3.3	Computer setup . . . . .	36
3.4	Java included libraries . . . . .	40
4.1	Database parameters . . . . .	41
5.1	Parameters that are stored in the database . . . . .	54



# List of Algorithms

2.1	Generation of OBU specific keys . . . . .	27
2.2	Generation of session keys . . . . .	28
2.3	Generation of <i>MAC-1</i> and <i>MAC-2</i> . . . . .	29



# Listings

2.1	AutoPASSdata1 . . . . .	13
2.2	AutoPASSdata2 . . . . .	13
2.3	AutoPASSdata3 . . . . .	14
2.4	Example of a type 1 price record . . . . .	19
2.5	Example of a type 2 price record . . . . .	20
2.6	Example of a type 3 price record . . . . .	20
2.7	Example of a type 4 price record . . . . .	21
2.8	Example of a price file . . . . .	21
2.9	Example of a currency file . . . . .	22
2.10	Example of an operator file . . . . .	23
2.11	Example of a blacklist file . . . . .	23
2.12	Example of an exception file . . . . .	24
3.1	SQL syntax for the AutoPASS table . . . . .	38
B.1	DES weak keys. From [21] . . . . .	77



# Glossary

AutoPASS	The Norwegian automatic toll-collection system.
Ciphertext ( $C$ )	Symbol representing encrypted data.
DES	Data Encryption Standard (FIPS PUB 46).
$\gcd(a,b)$	Greatest common divisor of $a$ and $b$ .
LUCIFER	Cryptographic cipher and predecessor of DES.
MB	megabyte. $1 \text{ MB} = 10^6$ bytes.
MiB	mebibyte. $1 \text{ MiB} = 2^{20}$ bytes.
Plaintext ( $P$ )	Symbol representing unencrypted data.
ppm	Parts per million.
RSA	Public key cryptographic algorithm. Named after the authors R. <b>R</b> ivest, A. <b>S</b> hamir, L. <b>A</b> delman.
Vignette	A form of road pricing.
$\oplus$	The exclusive OR logical operation.





# Acronyms

**ALPR** Automatic License Plate Reader.

**ASECAP** Association Européenne des Concessionnaires d'Autoroutes et d'ouvrages à Péage (European Association with tolled motorways, bridges and tunnels).

**BST** Beacon Service Table.

**CESARE** Common Electronic Fee Collection System for an ASECAP Road Tolling European Service.

**CPE** Charging Point Equipment.

**CS** Central System.

**DES** Data Encryption Standard.

**DSRC** Dedicated Short-range Communication.

**DST** Daylight Saving Time.

**EEA** European Economic Area.

**EETS** European Electronic Toll Service.

**EFC** Electronic Fee Collection.

**ETC** Electronic Toll Collection.

**EU** European Union.

**GUI** Graphical User Interface.

**GVWR** Gross Vehicle Weight Rating.

**IDE** Integrated Development Environment.

**JPEG** Joint Photographic Experts Group.

**MAC** Message Authentication Code.

**MITM** Meet in the Middle.

**NDPA** Norwegian Data Protection Authority.

**Norvegfinans** Norske Vegfinansieringsselskapers Forening.

**NPRA** Norwegian Public Roads Administration.

**NTNU** Norwegian University of Science and Technology.

**OBU** On-Board Unit.

**OCR** Optical Character Recognition.

**PAN** Personal Account Number.

**PMC** Charging Point Main Computer.

**RFID** Radio-frequency Identification.

**RSE** Road-side Equipment.

**RSU** Road-side Unit.

**VST** Vehicle Service Table.

# Chapter 1

## Introduction

Riksrevisjonen published a report 11. December 2012 concerning their investigation of the Norwegian toll sector [32]. The report concludes that the automation of the sector has significantly contributed to making the toll payment process more convenient for the users. The same report also stress that the levying of toll is not carried out at the lowest possible cost. Riksrevisjonen points out that the operating costs for 2011 was 12.5% of the total toll collected which amounts to 818 million NOK. Other remarks include significant losses on receivables due to unpaid claims and a costly image processing procedure due to vehicles passing without a tag.

AutoPASS is one example of a system that produces a lot of data that, if combined and structured in the right way, can reveal a lot about an individual. The anonymity provided by such dynamic systems presents a problem [30]. On one hand this modernization is a good thing - it speeds up the whole payment process and simplifies the process of paying for the usage of a transport service. On the other hand this transaction produces an entry in a database. When your car equipped with an AutoPASS tag passes a toll station, your subscription is identified by reading the tag and you are billed accordingly. Even though a system such as AutoPASS lacks the ability to identify the persons in the car, it is fair to assume that the car was driven by the owner of the AutoPASS account or other individuals in that persons circle of acquaintances with access to the car.

### 1.1 Previous work

A study on the privacy-related issues in dynamic systems such as AutoPASS was the topic of [30]. This thesis concludes that there are challenges related to user privacy and that work needs to be done on the legislative side to improve the privacy. Large

scale data analysis can have a negative impact on user privacy as systems, such as AutoPASS, gain more subscribers and the amount of stored data grows.

## 1.2 Tolling in other countries

On what grounds road toll is collected vary between countries. Some countries, like Norway and Spain, may charge you relative to the road section. In Austria you are required to buy a Vignette where you pay for a certain amount of time, and not per road section. Evidence of payment is often realized as a visible toll sticker that is attached to the vehicle. Some countries also levy a special city toll, toll for using tunnels and toll on bridges. Many countries have adopted their toll road systems to become more automated. Examples are the 407ETR in Canada (<http://www.407etr.com/>), eFlow in Ireland (<http://www.eflow.ie/>), and TELEPASS in Italy (<http://www.telepass.it/>) to name a few. All the former systems use a transponder located in the car that communicate with the toll plaza when passing.

## 1.3 Aim of this thesis

As Riksrevisjonen points out, money is lost due to cars not being identified. The Norwegian minister of transport and communications, Marit Arnstad, has indicated as a response to Riksrevisjonen's findings that a bill proposal to introduce mandatory AutoPASS tags in vehicles above 3.5 tonnes is out on hearing [32, p. 18]. One could imagine that mandatory tags for all vehicles on Norwegian roads is the next step. This will produce vast amounts of data. Grouping this data together can reveal information about a specific individual that might violate the right to privacy. One goal of this thesis is to get a better understanding of how the AutoPASS system is built up with respect to anonymity. A path that will be investigated is the possibility to use anonymized traffic statistics to aid in the process of identifying cars. The rationale is that if one, or a specific group of toll plazas, stand out with respect to the number of unidentifiable transactions, one can target the efforts toward these plazas. As an example of the above, look to the area of public transportation. Bus companies perform manual controls to uncover people who do not pay - it is an interesting question if this is something that could be employed in the toll road sector. To investigate the problem further, a simulator is set up. To limit the area of focus, the group of toll plazas that make up Miljøpakken in Trondheim are selected. The simulator generates transactions at these toll plazas and stores them in a database. A program is to be developed to process the data and reveal the statistics.

## 1.4 Outline

The first chapter covers the background for toll levying in Norway and the AutoPASS system. This is meant to provide an insight into the current protocols for registering vehicles. Next, the reasoning and setup of the simulation and generation of statistics are described. In the following chapter the results of the simulation are shown. The applicability is discussed next, along with the anonymity issues in AutoPASS, before the thesis is concluded.



# Chapter 2

## Background

### 2.1 AutoPASS in a nutshell

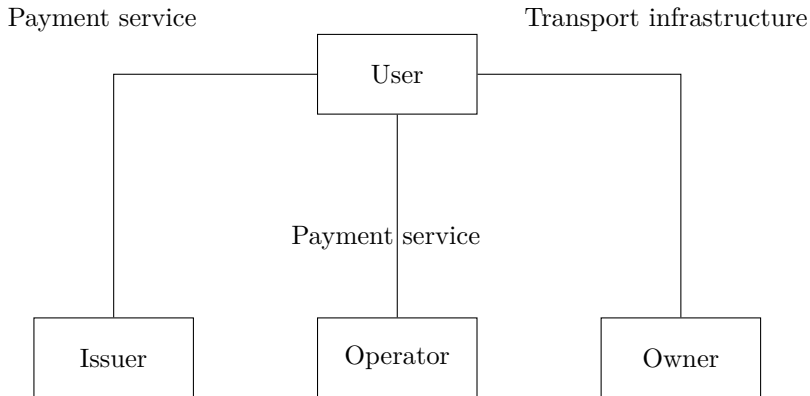
What AutoPASS provides is a service that allows the user to pay for the usage of transport infrastructure. Examples include toll charges on bridges, tunnels, and roads - one can even use the AutoPASS system on certain ferries in Scandinavia, including the Flakk-Rørвик ferry connection in Sør-Trøndelag. What AutoPASS adds is a service that allows seamless payment - the payment process is sped up by paying for the service without even stopping the car and the payment system is accepted by many transport services.

First the user is set up with a central account and given an AutoPASS tag. This tag can be either a smart card or a Radio-frequency Identification (RFID) device placed in the vehicle. In the smart card case, the user is required to present the card to a machine or a cashier at the point of usage. The payment process can be done without stopping if the RFID tag is used. The tag is attached to the inside of windshield and when the car is passing the toll lane the tag is read and the user is subsequently charged, either by deducting pre-paid money from the user's account or by sending an invoice.

### 2.2 Administrative outline of AutoPASS

#### 2.2.1 Actors

Figure 2.1 shows the actors that make up the general model for the AutoPASS system. You, as a user, want to use a transport service provided by an owner. To use that particular transport service, for example a bridge, tunnel, or ferry, you have to pay



**Figure 2.1:** Actors in the AutoPASS system

a fee. To collect these fees, the owner has put up charging points (or toll plazas) that are administered by an operator. You, as the user, enter into a contract with an issuer that provides you with a central account and a tag. When the operator logs you at the charging point, a claim is forwarded to your issuer for the  $x$  amount of money you need to pay for using the transport infrastructure. Your issuer then fulfills the claim forwarded by the operator, meaning that it pays the  $x$  amount of money on your behalf. This scheme works even if the operator and issuer are two separate toll road companies as the AutoPASS system ensures interoperability by enforcing standards.

The division outlined above can be made even more specific by an example. The Norwegian Public Roads Administration (NPRA) owns the AutoPASS system as a whole. They are responsible for the requirement specifications, choosing the equipment and making deals with the vendors. The transport infrastructure, like a bridge, tunnel, or road, is administered by the NPRA on behalf of the government. Toll road companies have the right to levy toll for a specific project. Examples of such companies are Eikesundsambandet AS, Nord-Jæren Bompengeselskap AS, and Bergen Bompengeselskap AS. The toll company can operate and manage the payment service themselves or they can outsource it. Companies such as Bro & Tunnelselskapet, Fjellinjen, and Vegamot, represent operators that maintain the payment service. Note that some of the latter companies are also a toll road company, not just a payment-service provider.



### 2.2.2 Legal background

The legal grounds for levying toll in Norway is found in Veglova §27, which states that the Ministry of Transport and Communications (Samferdselsdepartementet), on approval from the Parliament (Stortinget), can introduce toll on public roads in Norway [23]. AutoPASS as a whole is owned and administrated by the Norwegian Public Roads Administration (Statens Vegvesen). A number of contracts are signed as part of the toll road process. An introduction to some of the contracts is given below.

#### *Bompengeavtalen*

Bompengeavtalen is a legal contract between the toll road company and the government represented by the NPRA. A standardized text forms the basis for this contract and it is signed when the Parliament has approved the toll project. The signing of the contract marks the point where the toll road company can start to levy toll. The contract clarifies each party's responsibilities in the toll road project. As an example, the NPRA manages the construction and the toll road company finances a percentage of the build to the extent indicated in the contract. Depending on when the levying of toll starts, the toll company may need to take out loans to finance the construction - this is how the toll company is able to finance the build when the levying of toll starts after the project is finished and opened to traffic. The toll company administrates the loan until it is repaid and enough money to terminate the operation is collected. The maximum duration for a toll road project is set to 15 years, with a possibility of being granted five more years by applying to the NPRA and Vegdirektoratet. A template of this contract can be found in [39, enclosure 1].

#### **AutoPASS user contract**

As a new user to AutoPASS you need to enter into a contract with an issuer to provide you with a central account and an AutoPASS tag. The issuer is responsible for initialization of the tag and is also responsible for this tag to other AutoPASS operators. All AutoPASS users have access to the same general agreement, but there are openings to enter into special agreements, for example where the operator is also an issuer and is able to offer rebate on prepaid fares in its own toll plazas. If you as a user enter into a contract with Trøndelag Bomveiselskap, you can get 30-50% rebate on fares in toll plazas between Trondheim and Stjørdal. The amount of rebate is dependent upon the number of prepaid fares. If you do not have this type of contract, but still an AutoPASS tag, your issuer will be billed for the full price. Your issuer

will subsequently deduct this amount of money from your account or send you a bill at a predetermined interval.

### **AutoPASS issuer contract**

This contract is for companies that want to become AutoPASS issuers. Committing to this contract gives you the ability to issue tags. The responsibilities of an issuer have been mentioned earlier - these include managing the central account and pay claims from other operators.

### **AutoPASS joint venture contract**

This is a contract between the operators, owners of infrastructure, and the service providers. As an example, a toll company that signs this contract is committed to deliver a transport- and payment service compatible with the AutoPASS system.

## **2.3 Technical background**

### **2.3.1 Standards and directives**

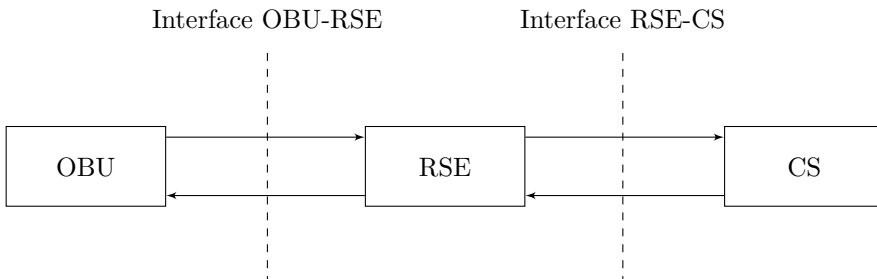
The AutoPASS platform builds on a set of specifications set forth by the NPRA. On the European level there is an interoperability initiative called Common Electronic Fee Collection System for an ASECAP Road Tolling European Service (CESARE) set up by Association Européenne des Concessionnaires d'Autoroutes et d'ouvrages à Péage (European Association with tolled motorways, bridges and tunnels) (ASECAP) with the goal of a common inter-operable Electronic Fee Collection (EFC) system in Europe. Norway is represented in ASECAP by Norske Vegfinansieringsselskapers Forening (Norvegfinans). AutoPASS and its specifications are based on recommendations by ASECAP and system requirements from CESARE projects [18].

For an EFC protocol to receive widespread adoption and interoperability between countries, some form of common understanding of how the system shall behave is needed. NS-EN ISO 14906:2011 - Electronic fee collection - Application interface definition for dedicated short-range communication is such a standard meant to 'provide the basis for agreements between operators, which are needed to achieve interoperability' [17]. Also worth mentioning is BS-EN 15509:2007 - Electronic fee collection - Interoperability application profile for Dedicated Short-range Communication (DSRC). The European Union (EU) also pass directives which impacts Norway

as a part of the European Economic Area (EEA). Directives of relevance include the EFC directive [16] and the European Electronic Toll Service (EETS) decision [15].

### 2.3.2 AutoPASS system

This section is meant as a technical introduction to the AutoPASS system. The entities that will be introduced in this section include the On-Board Unit (OBU), the Road-side Equipment (RSE), and the Central System (CS).

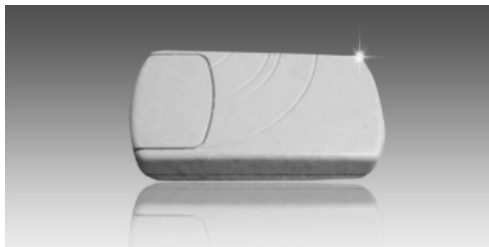


**Figure 2.2:** Nodes in the AutoPASS system

Figure 2.2 shows the nodes covered in this section, including the interfaces between the nodes.

### 2.3.3 On-board unit

The OBU is located inside the vehicle, typically attached to the windshield [10]. It partakes in the transaction that takes place when the vehicle passes the toll plaza. The OBU, or sometimes also just *tag*, serves as a token representing the user and the AutoPASS contract.



**Figure 2.3:** Norbit ITS FZ2358 OBU. The image is taken from datasheet [27].

Figure 2.3 shows an example of an OBU.

### 2.3.4 Road side equipment

The Charging Point Equipment (CPE) is a collective term used about the systems and modules placed roadside that make up the 'tool booth'. This includes the system you see over the lane as you drive through but also the storage- and processing unit stored close nearby.



**Figure 2.4:** Figure of RSE near Sluppen bru in Trondheim

In figure 2.4 you see an example of a roadside setup. The cameras are placed so that they can capture both the front and rear license plates. Over the two lanes one can see the DSRC units. Immediately after the lane one can see the light-signal boxes. The house on the left is the facility where the roadside processing unit is located. Transaction logs destined for the central system are stored here until they are transferred.

### 2.3.5 Central System

The central system receives and stores information collected from the roadside equipment. Transaction data generated by vehicles passing the toll plaza are sent from the roadside system to the central system. *CS Norge* is the name for the central system, and the system is developed by *Q-Free* [28].

### 2.3.6 Interface on-board unit - charging point equipment

The OBU and the RSE are the two first entities that communicate in an AutoPASS transaction. The part of the RSE that is being used for communication with the OBU is termed Road-side Unit (RSU). Let's cover some of the metrics on the radio link first.

#### Radio Link

The radio link is set up as channels in the 5.8 GHz band. Four downlink carrier frequencies (RSU to OBU) exist - 5.7975 GHz, 5.8025 GHz, 5.8075 GHz, and 5.8125 GHz [36], where the two latter frequencies are allocated on a national basis. The uplink channels (OBU to RSU) are realized as a sub-carriers on either 2.0 MHz or 1.5 MHz, where a spacing of 1.5 MHz is recommended for interoperability with existing installations [35]. The downlink and uplink bit rate are 500 kbit/s and 250 kbit/s respectively. The limit for power varies depending on the subcarrier-shift. The limits are -17 dBm\* for 1.5 MHz and -24 dBm for 2.0 MHz. The lower limit is -43 dBm and the OBU cuts off (no communication) if the signal strength drops below -60 dBm [35]. Doing the conversion from dBm to mW gives a power output of

$$-17 \text{ dBm} = 20 \mu\text{W} \quad (2.1)$$

$$-24 \text{ dBm} = 4 \mu\text{W} \quad (2.2)$$

To save power, the OBU is sleeping when not in use and is triggered to wake up if it receives data. [35] gives 11 as the number of octets required for wakeup, but stress that it can also be less. No special pattern is required. From the point the OBU receives the trigger, the wake up time should be  $\leq 5$  ms [35]. There is also a given tolerance for the drift in frequency. For the downlink the tolerance is set to  $\pm 5$  ppm (= 0.0005 %) and  $\pm 0.1$  % on the sub carriers [35]. The AutoPASS standard explicitly states in requirement R-Link1-13 that an RSU shall handle a Doppler shift of at least  $\pm 1000$  Hz [7].

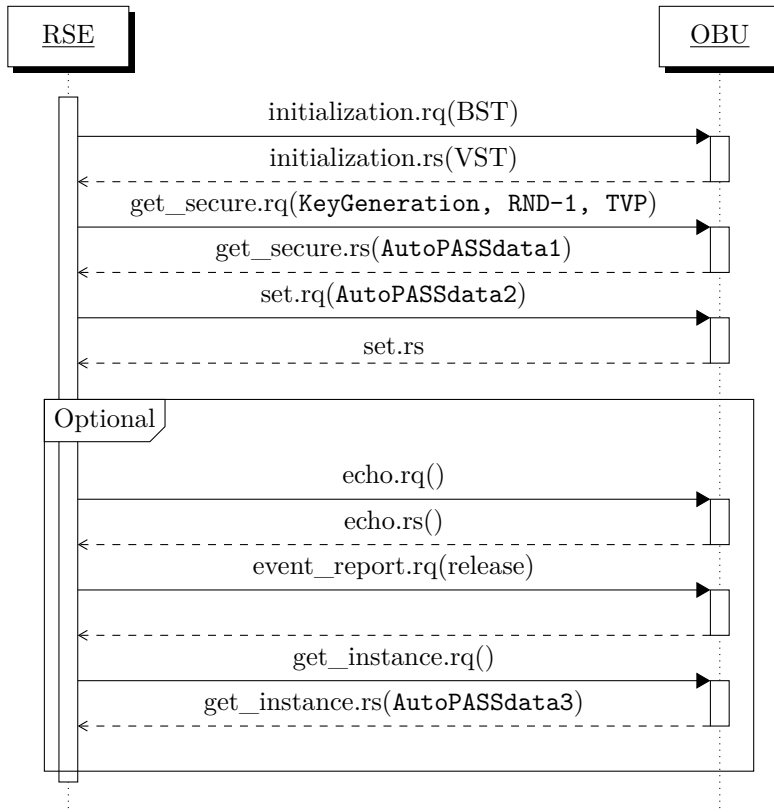
To put this into perspective, imagine that the two radios are in-sync with respect to frequency. A car driving through the toll plaza at speed will introduce a Doppler shift, where the received frequency will shift up or down depending on the relative speed and direction. Let's assume channel 1 is being used (5.7975 GHz). This gives a maximum speed in the order of 51.7 m/s ( $\approx 186$  km/h). The calculations are given in appendix A.

---

\* dBm is used to show the measured power in reference to 1 mW on a decibel scale. 0 dBm is therefore 1 mW. 3 dBm is 2 mW, and so on.

### Message exchange

The sequence of exchanged messages are sought illustrated in a sequence diagram in figure 2.5.



**Figure 2.5:** Sequence diagram showing the messages exchanged between the on-board unit and the road-side unit. From [7].

The Beacon Service Table (BST) is periodically broadcast from the RSU. The BST includes `manufacturerID`, `individualID`, `time`, and `profile`. The two IDs are set by the manufacturer. The `time`-variable represents real time as a 32 bit UNIX timestamp, and `profile` represents the subcarrier-profile supported by the RSU.

Upon receiving the BST, the OBU responds with the Vehicle Service Table (VST) if any matching `profiles` are found. The VST includes confirmation of selected `profile`, OBU link address, data on issuer of the tag labeled `manufacturerId`, a sequence of flags called `efcStatus` where only `OBUmoved` and `batteryLow` are in use

for AutoPASS. An EFC-ContextMark is included and contains information about active subscriptions.

Upon receiving the VST, the RSU initiates a `get_secure` request. The request is addressed to the link address of the OBU and contains an integer designating which key generation method to use, `keyGeneration`, 4 octets of random numbers, `RND-1`, and 4 octets with a time variable parameter to be used as freshness in Message Authentication Code (MAC) generation, `TVP`. When the OBU receives the request, a `get_secure` response is sent back to the RSU.

```

AutoPASSdata1 ::= SEQUENCE {
  obuID CS1 [9],
  efcStatus BIT STRING (SIZE (16)),
  TC OCTET STRING (SIZE (2)),
  RND-2 OCTET STRING (SIZE (4)),
  MAC1 OCTET STRING (SIZE (4)),
  MAC2 OCTET STRING (SIZE (4))
  LogIndex INTEGER (0..255)
}

```

**Listing 2.1:** AutoPASSdata1

The enclosed information in the response is shown in figure 2.1 called `AutoPASSdata1`. The `obuID` is a concatenation of three separate identifiers, according to a standardized data format named CS1 [37]. The ID is 56 bits long (7 octets), where `CountryCode` makes up the first 10 bits, `IssuerIdentifier` makes up the next 14 bits, and the last 32 bits are given by the `ServiceNumber`. `efcStatus` is mentioned earlier, holding `OBUmoved-` and `batteryLow` flags. `TC` is the transaction counter stored locally on the OBU which is 16 bits. `RND-2` is a random number generated by the OBU. `MAC-1` and `MAC-2` are results of a MAC operation using the `KeyGenerationNumber-` and `time` variables received in the BST-message, `RND-1` received in `get_secure.rq`, the `obuID`, `OBU status`, and `RND-2` generated in the OBU. `LogIndex` is a pointer to the last entry on record in the OBU.

```

AutoPASSdata2 ::= SEQUENCE {
  LogIndex INTEGER (0..255),
  OBUstatusControl OCTET STRING (SIZE (2)),
  passingLogData AutoPASSdata3
}

```

**Listing 2.2:** AutoPASSdata2

```

AutoPASSdata3 ::= SEQUENCE{
LogType INTEGER(0..255),
SessionTime TimeReal,
SessionServiceProvider Provider,
StationLocation INTEGER(0..1048575),
SessionLocation BIT STRING(SIZE(8)),
TypeOfSession StationType,
SessionResultOperational ResultOp,
SessionResultFinancial ResultFin,
ReceiptAuthenticator OCTET STRING(SIZE(2))
}

```

**Listing 2.3:** AutoPASSdata3

After receiving the `get_secure` response, the RSU wants to store a receipt of the transaction on the OBU. The data are sought written to the `LogIndex` pointer received from the OBU. The contents of the receipt are shown as `AutoPASSdata2` and `AutoPASSdata3` in listings 2.2 and 2.3 respectively. The OBU responds with `set.rs` as a confirmation that the log file is stored.

The RSU can track the OBU while inside the boundaries of communication. This is done by the `echo` request. The OBU answers with `echo` response. The RSE can instruct the OBU to terminate the transaction by issuing a `release` request. The receipts stored on the OBU can be retrieved by issuing a `get_instance` request. `posOfFirstInstance` and `posOfLastInstance` indicates the number of records to retrieve. Note that this query is not access restricted, meaning that anyone in principle can implement the protocol and read the receipts from the tag [29].

### 2.3.7 Interface charging point equipment - central system

The interface between the CPE and the CS facilitates the transport of transaction data from the CPE to CS and from CS to CPE.

Including the transaction related data; the RSE also sends picture files and exception messages to the CS. A number of files also travel the other way. The OBU status file is one example. It contains info on active OBUs such as the balance of the central account and validity of the contract.

An introduction to the various files is given below.



## Transaction file

Each charging point generates a transaction file which, at regular intervals, is transmitted to the central system. This transaction file holds records of variables such as the obuID, primitives such as RND-1, RND-2, MACs, the price that was charged, which light signals that were given to the driver, and OCR data. Every passage will create an entry in the transaction file and make its way into the central system when the transfer occurs, typically every 24 hours [8]. The transaction file is large in the sense that it holds over 70 fields for every transaction. An overview of the file is sought given in table 2.1.

Charging point related parameters (1-3)
Time related parameters (5-6)
Status parameters (8-10)
OBU identifier parameters (12-14)
Key- and security related parameters (16-27)
Sequence numbers (counters) (30-34)
Payment related parameters (28, 36-42, 49)
Lane- and signal related parameters (44-48)
Vehicle- and OBU related parameters including OCR (50 - 80)

**Table 2.1:** Overview of the transaction file sent from charging point equipment to the central system.

Charging point related parameters include the ID of the toll plaza that was passed, if the passing was in or out of a toll area, and the lane number. Time related parameters include the time in YYYYMMDDHHMMSSmmm format, for example 20130101000101000. A separate parameter indicates whether daylight saving time is used or not. The status parameters include the signal code, which is a textual representation of how the vehicle passed the toll plaza. An example is signal code #20 which states "Passage in AutoPASS lane with expired validity or passage, no value left, or OBU blacklisted" [8]. VehicleClass is a separate parameter indicating the type of vehicle. TagStatusFlag is related to the OBU status file which is sent from the CS to the CPE. The TagStatusFlag currently holds three flags, 'Wanted', 'Video', and 'Service'. If the OBU status file contains any of these flags, a predefined action will be performed and the corresponding flag will be set in the transaction file. If the 'Wanted' flag is set, it will trigger the camera to take a picture and send an exception to the central system. The 'Video' flag will also trigger the camera, and the 'Service' flag seems to be some sort of debugging mode that records additional information on the OBU communication - the specification does not say in detail what is saved in the latter

case [8]. OBU identifier parameters include the triplet used to uniquely identify an OBU, CountyCode, IssuerIdentifier, and ServiceNumber.

Key- and security related parameters include the KeyGeneration (KGN) parameter used to identify which generation of masterkey that is used, the random number generated by the RSE during the transaction, RND-1. The Time parameter contains the UNIX-time used to create the MACs. obuID is included and obuStatus contains flags for 'obuMoved' and 'batteryLow'. The transaction counter, TC, is an internal counter in the OBU that increase with every passage. The TC is 16 bits, so it will overflow when  $2^{16} - 1 = 65535$  passes is reached. The counter should then be reset to 0. RND-2 is a random number generated by the OBU. The obuID, obuStatus, TC, and RND-2 is needed to verify the MACs generated during the transaction as they, along with the secret keys, form the input to the MAC algorithm.

MAC1Status and MAC2Status indicate the result of the MAC verification roadside. #0 indicate 'not checked', #1 indicate 'checked, approved' and #2 indicate 'checked, not approved'. The MAC1 and MAC2 fields hold the specific message authentication codes. Even though both MAC1 and MAC2 are sent in every transaction, it is not always possible to check MAC1 roadside. To verify MAC1 one would need the masterkey held by the issuer of that OBU, and this key should be kept private. MAC2, on the other hand, is intended to be verified by knowledge of a *foreign* masterkey. The key structure of AutoPASS will be covered in subsequent sections. The requirement specification states that if any disputes occur, for example if MAC2 does not verify but MAC1 does, MAC1 is regarded as proof as it is verified by the operator and responsible issuer of the OBU [9]. SignalLevel indicates the OBU performance.

The next section holds a number of counters. SeqValidPayment indicates the number of passages that was valid, SeqEnforced counts the number of situations where no payment was made, for example if no OBU is registered, or no payment is made in a manual lane. SeqCPETransaction counts every transaction sent from the CPE. SeqVideoPicture counts the pictures sent from CPE to CS, for example pictures taken if no OBU is registered, or if either the 'wanted', 'video', or 'service' flags are set in the TagStatusFlag, or post-payment by invoice. Test-images taken by the cameras will not be included in this counter.

Payment related parameters hold parameters related to manual passages. TypeOfPayment specifies the payment medium for manual passages, for example #02 Credit Card or #01 Cash. For other passages the default value is 00. TypeOfCreditCard, CreditCardNumber, CreditCardExpiry, and CreditCardSequenceNo are related to payments with credit card. Some of the fields are used for secondary purposes - if credit card payment is not used, CreditCardNumber holds the KID-number in case

of invoice payment. CreditCardExpiry hold the reason for 'Free passage' in a manual lane, for example '0005 Funeral Procession' or '0002 Emergency'. MoneyBagNumber holds the number of the bag used in the manual lane at the time.

The first parameter among Lane- and signal related parameters is a SignalCodeBitmap, indicating signals given during the transaction. Examples include 'OBU not read', 'OBU not detected', 'OBU not authenticated'. LaneMode shows how this lane was used at time of passage, for example if it was an AutoPass lane (#01), manual lane (#02), free passage lane (#04). LightSignalCode holds the code for the light signal presented after the transaction, with three possibilities, 'Green', 'White', and 'Amber', indicating 'Approved passage', 'Low balance passage', or 'Invalid passage' respectively.

The last block contains Vehicle- and OBU related parameters. First there is a record of the validation file used for OBU verification. If the OBU is blacklisted the name of the blacklist is given, otherwise the name of the OBU status file is used. Next is a series of special parameters used for classification. Special parameters include the measured length, measured weight, number of axles, special classification code, number of passengers, measured width, and measured height. Optical Character Recognition (OCR) parameters include data related to the vehicle's license plate. Pictures are taken of both front and rear license plates. The OCR process returns the following, for both front and rear camera: License plate number, nationality of license plate, OCR confidence, and OCR group. The confidence is produced by the OCR process and graded from 0 – 100, where the higher number indicates a higher degree of confidence. OCR group is produced by the OCR function and indicates the final result of the process, for example #0 Confident result, #1 Image with no license plate number, or #3 need manual assistance. Results from both front- and rear views are aggregated together and produce the following parameters: License plate number (front and rear), nationality of license plate (front and rear), OCR confidence (front and rear), and OCR group (front and rear). The difference from the previous parameters is found in the OCR group, where a comparison is done between the front- and rear readings. #0 Confident OCR result indicates that the readings were found to match, #1 Image with no license plate indicate that no license plate was found on either the front, rear, or both places. #2 need manual assistance on the front, rear, or both places. #3 license plate mismatch between front and rear reading. #4 possibly foreign license plate.

The last parameters in the transaction file are related to the European standard EN 15509 concerning interoperability. EN 15509 has a number of parameters stored on the OBU. Examples are vehicle class, vehicle dimensions, vehicle axles, vehicle weight limits, vehicle specific characteristics, equipment OBU id, and equipment status.

The reconciliation record is the last record in the transaction file. It contains the charging point ID, the time and the number of records on file, excluding the reconciliation record itself.

### OBU status file

The OBU status file holds parameters concerning a specific OBU and is sent from the central system to the roadside system to take part in the transaction. The contents of the file are shown in table 2.2.

Record type	Indicating the purpose of the OBU record, for example if it is to be deleted, updated, or is just a new record
OBUCountryCode	ISO country code. For Norway the code is 'NO'
OBUIssuerIdentifier	Identifier of the OBU issuer
OBUServiceNumber	Holds the OBU serial number
TypeOfContract	Indicates what type of contract is used - pre-paid or free passages contract
VehicleClass	Description of type of vehicle
StatuslistFlag	Flag indicating that a special function should be executed on a passage of this OBU
Validity	Indicating when the time-based contract expires
Balance	Amount of money in the central account
Override	Instruct the CPE to handle the transaction based on #1 validity and balance parameters or #2 based on the field in SignalCode
LightSignalCode	Holds the parameter of what light signal should be given
FareInformation	For future use
LicencePlateNumber	Holds the license plate number of the vehicle registered with the OBU
LicencePlateNationality	Holds the nationality of the license plate number

**Table 2.2:** Overview of the OBU status file parameters.

## Price file

The price file holds information on the amount to be charged for a passage. Price files can be differentiated; examples include type of vehicle, time of the day, day of the year, and lane. There exist four types of price records that can be present in a valid price file.

**Type 1** A record of type 1 holds what you would expect from a price file, namely price information. The format is shown in table 2.3.

Record type	Indicates type of record - for type 1 records this is set to 1
CP ID	ID uniquely identifying the charging point
Lane ID	Indicates the lane ID for which the record is valid
Lane type	Indicates what type of lane the price is valid for. One can differentiate between AutoPASS lanes and manual lanes
Vehicle class	Indicates what type of vehicles classes the file is valid for
Week day	Indicates which days the price is valid. '0,1,6' means that the price is valid for 'Sunday, Monday, Saturday'
Month	Indicates the month the price is valid
Day of month	Used together with 'Month' to cover pricing on specific days
Time	Specifies hours of the day when the price is valid. '15' means that the price is valid from 15:00
Min	Used to specify the minutes in an hour in which the price file is valid
Price	Five characters are used to represent the price in the range from 0 NOK to 99999 NOK

**Table 2.3:** Parameters in a type 1 price record

```
1 033 01 * * * * * * * * 00005
```

**Listing 2.4:** Example of a type 1 price record

A valid price record of type 1 is shown in listing 2.4. The line tells us that this is a type '1' record for charging point '033' and valid for lane '01'. It is also valid for all

lane types, all vehicle classes, on every day of the week, month, and day of month, at every hour and minute of the day. The price is set to '5' NOK.

**Type 2** A type 2 record shows the date from which the records of type 1 are valid. Table 2.4 shows the parameters in the file.

Record type	Indicates type of record - for type 2 records this is set to 2
ValidFromDate	A date specifying from when the price file is valid. Format YYYYMMdd

**Table 2.4:** Parameters in a type 2 price record

```
2 20130101
```

**Listing 2.5:** Example of a type 2 price record

A valid type 2 record is shown in listing 2.5, indicating that it is a type '2' price record and valid from January 1<sup>st</sup> 2013.

**Type 3** A record of type 3 is the last record in the price file and it holds a parameter indicating the number of records on file, excluding itself.

Record type	Indicates type of record - for type 3 records this is set to 3
Number of records on file	The number of records on file

**Table 2.5:** Parameters in a type 3 price record

```
3 15
```

**Listing 2.6:** Example of a type 3 price record

A valid type 3 record is shown in listing 2.6, indicating that it is a type '3' record and that the price file holds 15 records in total, excluding this record of type 3.

**Type 4** A record of type 4 indicates when the price file was created, and is placed first in the price file

Record type	Indicates type of record - for type 4 records this is set to 4
Date when price file was created	Date indicating when the price file was created. YYYYMMddHHMMSS format

**Table 2.6:** Parameters in a type 4 price record

```
4 20130101000001
```

**Listing 2.7:** Example of a type 4 price record

Listing 2.7 is a valid record of type 4, indicating that the price file was created on January 1<sup>st</sup> 2013 at time 00:00:01.

An example of an entire price file could look something like the example shown in listing 2.8.

```
4 20130101000001
2 20130101
1 033 01 * * * * * * * 00005
3 3
```

**Listing 2.8:** Example of a price file

### Picture file and picture text file

The picture- and picture text file are sent from the CPE to CS. The images are coded in the Joint Photographic Experts Group (JPEG) format. The data included with the picture is shown in table 2.7.

The picture text file records also contain the SignalCode, along with a text describing the reason for taking the picture.

### Currency file

An example of a valid currency file is given in listing 2.9. Table 2.8 shows the parameters in a currency file.

A given conversion rate is valid from the time specified until it is replaced by a more recent timestamp. In listing 2.9 we see that 1 EUR amounts to 7.49 NOK from 21<sup>st</sup>

Time	Time formatted as <i>YYYYMMDDHHMMSSmmm</i>
DST	Indicate if Daylight Saving Time is used
CP ID	Charging point ID
Lane	The lane number that was used
SeqVideoPicture	Counter of the number of pictures taken that is to be sent to the CS
OBU ID	OBU ID
SignalCode	Code indicating the reason for taking the picture

**Table 2.7:** Parameters in a picture file

CurrencyTypeNumber	Standardized number for the currency. Examples are 578 for NOK, 840 for USD
CurrencyTypeAbbreviation	Standardized abbreviation for the currency, For example USD and NOK
Time	The time from which the conversion rate is valid, <i>YYYYMMDDHHMMSS</i>
ConversionRate	Conversion rate compared to NOK. Floating-point number with two decimals

**Table 2.8:** Parameters in a currency file

978	EUR	20130421000000	7.49
978	EUR	20130512000000	7.61
208	DKK	20130512000000	1.02

**Listing 2.9:** Example of a currency file

of April 2013 at 00:00:00, until it is replaced by a new conversion rate of 7.61 NOK for 1 EUR on the 12<sup>th</sup> of May 2013 at 00:00:00.

## Operator file

The operator file is used to grant access to and identify operators of a charging point.

An example of a valid operator file is given in listing 2.10 and the parameters of the file are given in table 2.9. The file contains three operators, but only two of the three have access rights, as the Active-flag for Kari Kristiansen is set to 0.



OperatorID	ID identifying an operator
Password	Password used for login with a given operator ID. The password is restricted to be only four characters long
Active	Variable determines if the operator ID can be used. #0 Not active, operator ID cannot be used, #1 Active, operator ID can be used to log in
Operator name	Variable length string indicating the name of the operator

**Table 2.9:** Parameters in an operator file

```
0001 1234 1 Nils Nilsen
0023 2255 1 Per Persen
0142 0912 0 Kari Kristiansen
```

**Listing 2.10:** Example of an operator file**Blacklist file**

Personal Account Number (PAN)	Unique number identifying the account
Rejection code	Example: '90 - OBU not valid, no reason given', '95 - OBU stolen'
Action code	Example: '01 - Reject the OBU'
Reserved	Reserved

**Table 2.10:** Parameters in a blacklist file

```
7033191234567890127 95 01 00000000
7033191234567457521 99 01 00000000
999999999999999999 00 00 00000002
```

**Listing 2.11:** Example of a blacklist file

Table 2.10 shows the parameters in an OBU blacklist file. Listing 2.11 shows an example of such a file. Notice the last record in the file. The first 19 bytes are set to 9s to signify that this is a reconciliation record. The last  $32 - 19 = 12$  bytes contain the number of records on file, excluding the reconciliation record itself. The first record blacklists PAN '7033191234567890127' with code '95 - OBU stolen' and action '01 - Reject the OBU'. The second record blacklists PAN '7033191234567457521' with

code '99 - OBU returned from customer because of OBU fault' with action '01 - Reject the OBU'

### Exception messages

Exception messages are sent from the roadside equipment to the central system. The messages are prioritized relative to the severity of the information in the message. Messages labeled 'Fatal' are coded as priority '1' and 'Information' messages are given the lowest priority code of '5'. The time when the message originated is included, along with the Daylight Saving Time (DST) field. ModuleNumber is the ID of the module that generated the message. UnitNumber indicates the unit the message holds information about. CategoryNumber is used together with ModuleNumber to uniquely identify a message. AlarmText is a readable description of the exception.

Charging point ID	ID identifying the charging point
Lane	Number indicating the lane. If the fault is not connected to a lane, 0 is used as value
Priority	Exceptions can be given a priority flag from 1-5, where the lower number indicates higher priority
Time	Time when the message was constructed. <i>YYYYM-MDDHHMMSSmmm</i> format
DST	Indicate if daylight saving time is enabled
ModuleNumber	Identifier for module where the message originated
UnitNumber	Identifier for type of unit
CategoryNumber	Code indicating the type of error
AlarmText	Textual representation of the error

**Table 2.11:** Parameters in an exception file

Table 2.11 lists the parameters in an exception message. Listing 2.12 shows an example. The message is from charging point '34600' and the priority of the message is set to '1' ('FATAL'). The time of message generation was 15<sup>th</sup> January 2001 10:24:30.123 (DST). The ModuleNumber that generated the message was '000001' and the UnitNumber was '01' indicating the 'Charging Point Main Computer (PMC)'. The textual description of the exception was 'Charging point main computer failure'.

```
34600 1 20010115102430123DST 000001 01 001 'Charging
point main computer failure'
```

**Listing 2.12:** Example of an exception file

### 2.3.8 Key hierarchy

As a car passes the toll plaza, the RSE has to know if this OBU is valid or not. If it is valid, the `obuID` should be stored and the account should be charged. If it is not valid, the cameras should be triggered to take pictures and handle the transaction accordingly. For this check to be performed roadside, the issuer responsible for the OBU has to provide the toll plaza operator with a key under which the MAC can be verified. Two set of keys are made, both a *native* and a *foreign* key. The foreign keys are distributed to other EFC operators so that they can validate OBUs from issuers other than themselves. The hierarchy of keys is shown in table 2.12.

Key type	Native	Foreign	Note
Masterkeys	MKEY-N (5)	MKEY-F (5)	5 generations of masterkey-pairs are derived. The foreign keys are distributed to other operators.
OBU specific keys	OBUEY-N (5)	OBUEY-F (5)	Keys to be placed on the OBU are derived from the masterkeys. A total of 5 keys of each type are created
Session specific keys	SSKEY-N (n)	SSKEY-F (n)	Session keys are derived from the OBU specific keys.

**Table 2.12:** Key hierarchy in AutoPASS. From [9]

### 2.3.9 Key generation

The masterkeys denoted MKEY-N and MKEY-F are created by a third party responsible for handling the keys. OBU keys are derived from the masterkeys and stored on the OBUs by the manufacturer. A total of five pairs are stored, one pair for each generation of masterkeys.

AutoPASS uses the Data Encryption Standard (DES) for calculating the message authentication codes and generating the OBU keys. A brief introduction to DES is given in appendix B. Triple-DES, or just 3DES, is used with two independent keys. The ciphertext and plaintext are computed as shown in equations 2.3 and 2.4, where  $P$  denotes the plaintext,  $C$  denotes ciphertext.  $E$  and  $D$  symbols encryption and decryption respectively.  $K_1$  and  $K_2$  are two independent keys. To obtain the

ciphertext, the plaintext is encrypted under  $K_1$ . The result is then decrypted under  $K_2$  and then encrypted under  $K_1$  again. To obtain the plaintext the ciphertext is decrypted under  $K_1$ , encrypted under  $K_2$ , and decrypted under  $K_1$  again.

$$C = E_{K_1}[D_{K_2}[E_{K_1}(P)]] \quad (2.3)$$

$$P = D_{K_1}[E_{K_2}[D_{K_1}(C)]] \quad (2.4)$$

## Masterkeys

The specification does not give a detailed outline on how the masterkeys should be generated, just a set of requirements. A subset of these requirements are sought summarized below [9].

1. Key generation mechanism shall be designed such that knowledge of one key does not compromise others.
2. Keys should be generated independently.
3. Check for weak keys should be performed.

The specification states that a proven hardware-based random number generator should be used to achieve these requirements [9]. Instead of relying on a software process to produce the numbers, a hardware-based number generator relies on input from a physical process. As an example, imagine that you will use the background noise received from an antenna as the physical phenomenon. The antenna acts as a *transducer* and transforms the radio waves into an electrical signal. The electrical signal is amplified and is transferred into the digital domain with an analog-to-digital (A/D) converter. If your process is behaving statistically random, and your conversion does not alter this fact, you have a random number generator based on a physical phenomenon. The emphasis on using a *proven* generator can be interpreted as meaning that one should use generators with wide acceptance in the cryptographic community.

## OBU keys

A total of 10 keys are generated and loaded onto the OBU, 5 native- and 5 foreign keys. The keys are generated by performing a triple-DES encryption on two permutations of the `obuID`. The two sub-keys,  $K_L$  and  $K_R$ , are concatenated to produce a 16 byte key. The algorithm for generating the OBU keys is shown in algorithm 2.1.

**Algorithm 2.1** Generation of OBU specific keys

Get the OBU ID (7 bytes)

Prepend OBU ID with 'FF' to obtain 8 bytes.

-> VAL = 'FF' || OBU ID    Ex.: ('FF AA BB CC DD EE FF GG')

Permute VAL to obtain PVAL    Ex.: ('GG FF EE DD CC BB AA FF')

A method to generate PVAL is shown below in JAVA syntax:

```
public static String rotate(String VAL) {
    String PVAL = "";
    for (int i = 0; i < VAL.length(); i++) {
        PVAL += VAL.charAt(VAL.length()-1-i);
    }
    return PVAL;
}
```

Compute the first part of the key,  $K_{LEFT}$

$K_L = EDE_{MKEY-N} (VAL)$

Compute the second part of the key,  $K_{RIGHT}$

$K_R = EDE_{MKEY-N} (PVAL)$

Concatenate the two keys to make OBUKEY-N

$OBUKEY-N = K_L || K_R$

To produce OBUKEY-F (foreign key), the same procedure is run with the foreign masterkey MKEY-F. The procedure is repeated for each 5 generations of masterkeys, producing a total of 10 OBU keys.

---

The obuID is padded and encrypted using 3DES with two independent keys. A masterkey is 16 bytes long, so two DES keys,  $K_1$  and  $K_2$ , are generated by splitting the masterkey into two 8 byte halves. After padding, the obuID is encrypted to form the 8 byte subpart,  $K_L$ , of the OBU specific key. The other 8 byte subpart,  $K_R$ , is made from doing the same encryption, but the padded obuID string is reversed.  $K_L$  and  $K_R$  are concatenated to form a 16 byte OBU specific key.

### Session keys

Generation of session keys is described in algorithm 2.2. One of the 5 OBU keys is chosen. A time-variant parameter of 16 bytes is built up from the RND-1 and TIME variables. The native- and foreign session keys are generated by an XOR of the TVP with the OBUKEY-N and OBUKEY-F respectively.

---

#### Algorithm 2.2 Generation of session keys

Generate the native session key:

Use OBUKEY-N(KGN) corresponding to the KeyGenerationNumber, KGN, agreed upon in BST/VST.

Set up the time-variant parameter - A total of 16 bytes:

-> TVP = RND-1 || TIME || RND-1 || TIME

Generate the 3DES session key from OBUKEY(n) and TVP

-> SSKEY-N = OBUKEY-N(KGN)  $\oplus$  TVP = SSKEY-N<sub>L</sub> + SSKEY-N<sub>R</sub>

Next, generate the foreign session key:

-> SSKEY-F = OBUKEY-F(KGN)  $\oplus$  TVP = SSKEY-F<sub>L</sub> + SSKEY-F<sub>R</sub>

The key has a total key-length of 16 bytes. The session key is often referred to as SSKEY-(N/F)<sub>L</sub> and SSKEY-(N/F)<sub>R</sub> which is the left and right subpart of the key, each 8 bytes long.

---

### 2.3.10 Message Authentication Code (MAC) generation

AutoPASS generates two message authentication codes, *MAC-1* and *MAC-2*. *MAC-1* is generated using the native session keys and *MAC-2* is generated using foreign session keys. The MAC process is built up as a block-chaining sequence, meaning that a block cipher is run in multiple stages and output from previous stages is used as input in the next stage. The variables used to make the MAC include the obuID, obu status, transaction counter, and a random number generated by the OBU, RND-2. The block chain works on 8 bytes at the time so the variables need to be concatenated and padded out with 0s to become a multiple of 8 bytes. The obuID is 7 bytes, obu status and the transaction counter account for 4 bytes, two each, and the random number, RND-2, is 4 bytes. Summing up, that gives a total of 15 bytes and 1 byte of padding 0s are needed.

The process of generating the MACs is shown in algorithm 2.3. The block chain operation is illustrated in figure 2.6. The MAC message  $M$  is split into two halves, where the first part becomes  $I_1 = D_1$  and the second part becomes  $D_2$ .

---

**Algorithm 2.3** Generation of *MAC-1* and *MAC-2*

$M = \text{OBUID} \parallel \text{OBU STATUS} \parallel \text{TC} \parallel \text{RND-2}$

Pad out to the right with '00' so that  $M$  is a multiple of 8 byte blocks

Ex.:  $M = \text{'AA BB CC DD EE FF GG' 'HH II' 'JJ KK' 'LL MM NN OO' '00'}$

The generation of the MAC is split into stages.

STAGE 0:

$I_1 = D_1$

STAGE 1:

$I_2 = \text{DES}_{K_1}[D_1] \oplus D_2$

STAGE 2:

$I_3 = \text{DES}_{K_1}[I_2]$

FINAL STAGE:

Output =  $\text{DES}_{K_1} [ \text{DES}_{K_2}[I_3] ]$

MAC = TRUNCATE [Output]\*

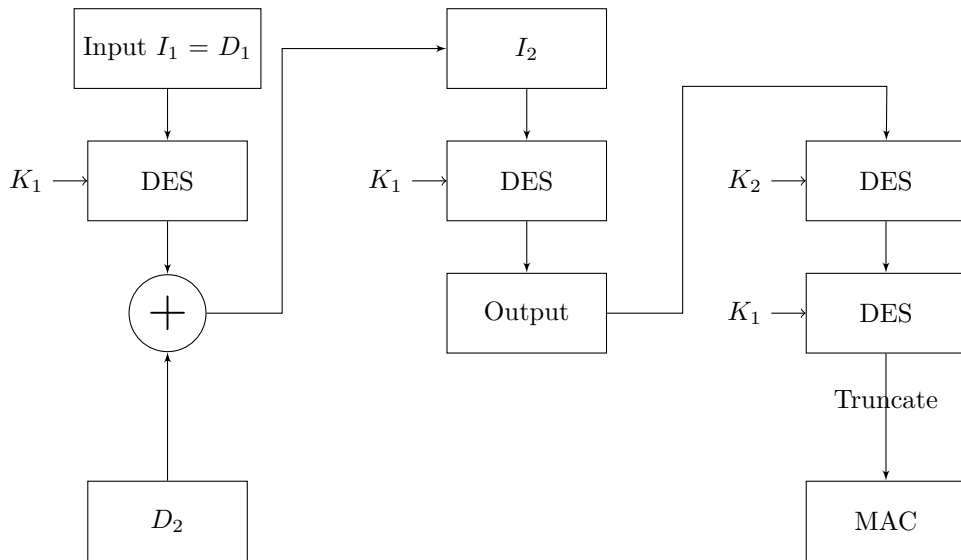
\* The output after the last DES operation is truncated, using only the 32 higher order (leftmost) bits, yielding a 4 byte MAC.

For MAC-1:  $K_1$ :SSKEY- $N_L$  and  $K_2$ :SSKEY- $N_R$  is used

For MAC-2:  $K_1$ :SSKEY- $F_L$  and  $K_2$ :SSKEY- $F_R$  is used

Increment transaction counter, TC.

---



**Figure 2.6:** Block diagram of MAC generation



# Chapter 3

## Methods

### 3.1 Outline

A major problem with AutoPASS is that if no OBU is present and the vehicle license plates are unreadable, for example after a heavy snowfall or a long dry period, identifying the vehicle is almost impossible. If the plates are unreadable by OCR they are sent to manual inspection. In such situations, even manual inspection by a human can prove difficult. Money is lost as the toll road company does not know where to forward the bill and the manual labor significantly increases operating costs. As a response to the findings presented in [32], the Norwegian minister of Transport and Communications has indicated that there is an ongoing effort to impose a mandatory AutoPASS OBU in every vehicle with a Gross Vehicle Weight Rating (GVWR) over 3.5 metric tonnes, starting with vehicles used for commercial purposes [32, p. 18]. The Norwegian data inspectorate implemented in February 2004 a licensing requirement for all automatic toll stations handling personal information. At the same time, they demanded an anonymous payment scheme [14].

The vast amounts of data produced in the system gives room for another approach to deal with the problem of people not paying. Anonymizing the traffic data and analyzing it to predict or show where the problem is most severe and target these toll plazas first. As an example, bus companies regularly have manual controls where representatives from the company or hired security officers perform the controls. Persons traveling with an invalid ticket are identified and issued a fine. An interesting question is whether the same thing can be done in the automatic tolling sector. The thought is to make an overview of these irregular passes and show them in a more graphical way.

These following sections will outline how statistics are to be used and how to generate sample data.

### 3.2 Statistics

To limit the scope of this prototype the simulation includes the toll plazas that make up what is known as *Miljøpakken* in Trondheim. Table 3.1 shows the location as well as traffic per day for these toll plazas. The data are collected before and after the toll plazas were put up, and changes in traffic volume is calculated in the rightmost column. The source of the data is [25].

<b>Toll point</b>	Before vehicles/24 hrs.	After vehicles/24 hrs.	Change vehicles/24 hrs.
Klett E6	23 400	<b>22 100</b>	1 300 (-6 %)
Klett Rv 707	8 300	<b>5 300</b>	-3 000 (-36%)
Bjørndalen	13 000	<b>8 400</b>	-4 600 (-35%)
Sluppen bru	23 000	<b>12 100</b>	-10 900 (-47%)
Kroppan bru	50 000	<b>50 500</b>	+ 500 (+1 %)
Nedre Leirfoss	5 000	<b>2 000</b>	-3 000 (-60%)
Være	13 000	<b>8 900</b>	- 4 100 (-32%)
<b>SUM</b>	<b>135 700</b>	<b>109 300</b>	<b>-26 400 (-19%)</b>

**Table 3.1:** Toll plazas in *Miljøpakken*. Data from [25].

The data in the *After*-column has been used to model the number of cars passing the toll station during 24 hours.

The charging system is built up such that vehicles above 3.5 metric tonnes pay twice as much as vehicles weighing in below that figure. Time-differentiated rates are also used, meaning that between 07 - 09 in the morning and 15 - 17 in the afternoon, a pass costs twice as much as it would normally cost. The exception is the toll plaza at Kroppan Bru - passes at this toll plaza are not time differentiated. Table 3.2 shows a comparison of the rates in the different toll plazas that make up *Miljøpakken*.

The time-differentiated cost means that the difference in traffic throughout the day becomes an important factor. The data presented in table 3.1 are *Miljøpakken* in Trondheim's own calculations. They present the data as *number of vehicles per 24 hours*. The traffic is not uniform during these 24 hours - people travel to work in the morning and home again in the evening. There are more cars on the road during the daytime. The point is that the number of factors that influence the distribution of cars are huge. Statens Vegvesen has developed a handbook for traffic calculations, handbook 146 [38]. In one of the examples they present the traffic distribution over 24 hours for Elgesetergate in Trondheim. This figure is shown as figure 3.1. The

	Kroppan bru	Kroppan Bru*	Others	Others*
Contract type	Per pass	Per pass	Per pass	Per pass
Base rate	5,-	10,-	10,- / 20,-	20,- / 40,-
prepay 2000,-	5,-	10,-	8,- / 16,-	16,- / 32,-
prepay 4000,-	5,-	10,-	8,- / 16,-	16,- / 32,-
prepay 7000,-	5,-	10,-	8,- / 16,-	16,- / 32,-
postpay private	5,-	10,-	8,- / 16,-	16,- / 32,-
postpay company	5,-	10,-	8,- / 16,-	16,- / 32,-

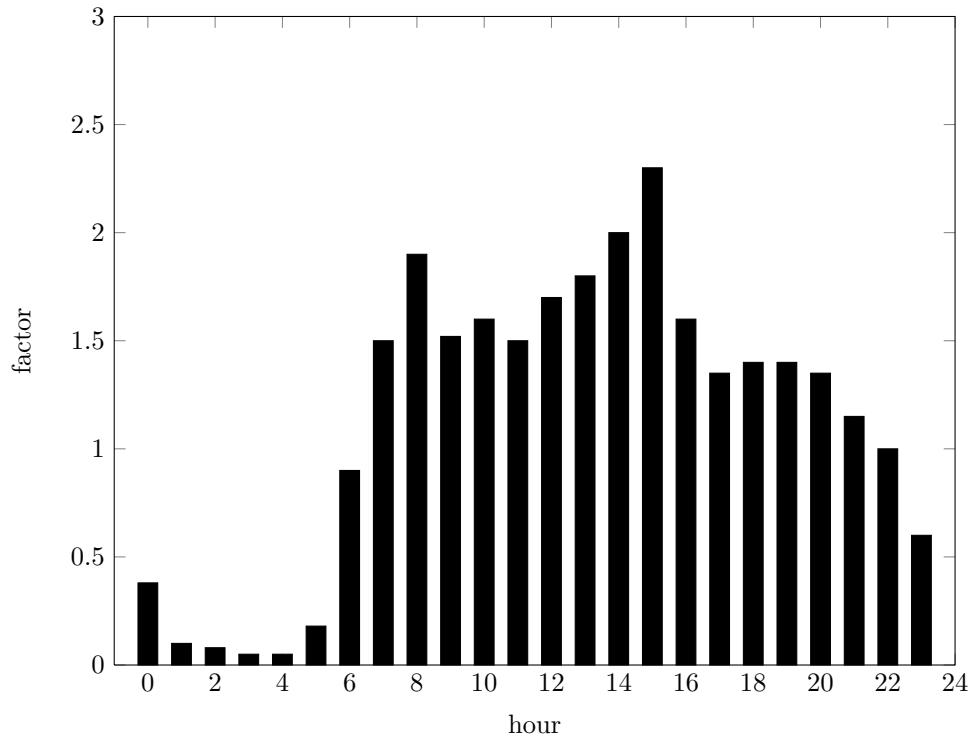
**Table 3.2:** Rates for the toll plazas in Miljøpakken. Values in NOK. From [11]. Columns with \* are for vehicles weighing over 3.5 metric tonnes.

figure is quite old, September 1983, but capture some of the elements mentioned above, namely how the traffic varies with people traveling to and from work. In addition, figure 3.2 has been used to model the weekly fluctuations in traffic.

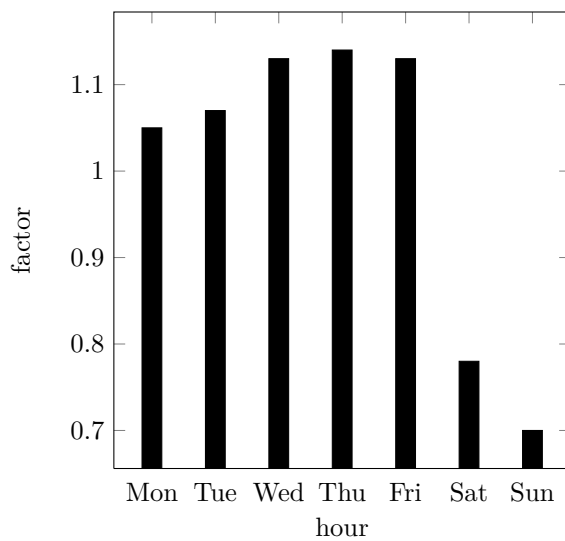
**Example 3.2.1.** In this example we will calculate the number of car passings at *Kroppan Bru* between 10:00 and 11:00 at a Wednesday. Using figure 3.1, we estimate that the hourly factor is 1.6. From table 3.1 we see that 50500 cars pass on a given day. This gives us  $\frac{50500}{24} \cdot 1.6 \approx 3366$  cars between hour 10 and 11. Spacing these out evenly over the hour gives  $\approx 0.935$  cars per second. Accounting for weekly fluctuations figure 3.2 is used. The factor for Wednesday is  $\approx 1.1$ . Multiplying in this factor gives us  $\approx 3703$  cars between the hours of 10:00 and 11:00. The number of cars is randomly distributed over the time interval [start, stop), where start in our case is 10:00 and stop is 11:00.

Another problem is how to model the percentage of cars that have an AutoPASS tag, and if they have one, how to set the probability of it working at the time of the transaction. The chairman of Trondheim Bomveiselskap was interviewed by adressa.no on the 6<sup>th</sup> of June 2013 about the fact that Miljøpakken is reaching 1 billion ( $10^9$ ) in collected funds. In the interview he gives a comment about tag-percentage in Trondheim, stating that 15 percent does not have an AutoPASS tag [2]. How this number is calculated was not explained. We can only assume that this is a good estimate for the number of vehicles with an AutoPASS tag. In the event that no AutoPASS tag is registered in the passage, and the subsequent license plate identification reveals that the vehicle is in fact registered with a valid AutoPASS subscription, the user's account is billed as if the AutoPASS tag was working.

The 15 percent failed AutoPASS transactions will trigger the cameras to take a picture and the OCR system will provide the license plate number. The Automatic



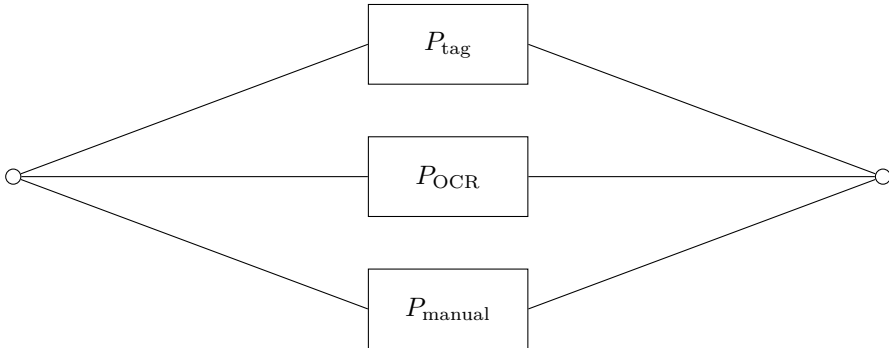
**Figure 3.1:** Graph showing model used to simulate traffic over a 24 hour period. Data from [38]. (reproduced)



**Figure 3.2:** Scaled weekly traffic patterns. Data from [40]. (reproduced)

License Plate Reader (ALPR) hit rate will vary. Weather conditions can greatly influence the readability of the license plates. A good estimation for the hit rate of such OCR systems seems to be around 95-98 % [3]. If the OCR fails, meaning that the front and rear results do not match or the result is just negative, the pictures are sent off to manual inspection. No viable statistics have been found for the manual inspection hit rate. It is therefore assumed that an operator, in the case where the OCR has not returned a confident result, is able to identify 50 percent of the vehicles.

Let us look at this from a reliability point of view, but first let us state the assumptions behind this model. The following analysis assumes that the AutoPASS tag, OCR system, and manual inspection fail independently. This is a simplification that might not hold in the real world, for example if the OCR fails, the manual inspection is more likely to fail. We identify that if the AutoPASS tag, the OCR system, or the manual inspection works we are able to identify the vehicle. The AutoPASS tag works with probability  $P_{tag} = 0.85$ . The OCR function works with probability  $P_{ocr} = 0.95$ . The manual inspection works with probability  $P_{manual} = 0.5$ .



**Figure 3.3:** Reliability of AutoPASS charging

This forms a parallel structure where each block represents the probability  $P_i$  that subsystem  $i$  is working. At least one of the subsystems must be working for the vehicle to be charged. We have that

$$P_{\text{working}} = 1 - \prod_{i=1}^n (1 - P_i) \quad (3.1)$$

$$P_{\text{failed}} = \prod_{i=1}^n (1 - P_i) \quad (3.2)$$

In the simulation, the probability of not being charged for the passage is therefore the probability that none of the subsystems are working

$$P_{\text{no charge}} = \prod_{i=1}^3 (1 - P_i) = (1 - 0.85) \cdot (1 - 0.95) \cdot (1 - 0.5) = 0.00375 \quad (3.3)$$

### 3.2.1 Scope of model

The model above is limited in scope - it does not capture every nuance one would see if real traffic data was used. When talking about traffic and traffic patterns it is customary to talk about hourly-, daily-, and annual variations. The model captures fluctuations in the traffic throughout the day as well as variations throughout the week. However, it is not concerned with variations throughout the year and increased traffic on days of the year when we normally see increased traffic, for example around the Easter holidays. As a direct result of that, the model fails to capture the reduced 'work traffic' in the summer months and around the Christmas holidays.

## 3.3 Setup

This section is dedicated to the hardware- and software foundation for the simulation.

### 3.3.1 Computer hardware

The hardware available has been one HP Compaq 8100 Elite SFF running Windows 7 and one HP Compaq dc7700p SFF running Xubuntu. Some of the hardware found in the two computers are listed in figure 3.3.

Component	HP Compaq 8100 Elite	HP Compaq dc7700p SFF
CPU	Intel i7 860 (2.80 GHz)	Intel Core 2 6400 (2.13 GHz)
Hard drive	500 GB, 7200 RPM SATA 3.0 Gb/s	160 GB, 7200 RPM, SATA 3.0 Gb/s
Operating System	Windows 7	Xubuntu 12.04.02 LTS

**Table 3.3:** Computer setup

### 3.3.2 Installation

The code for generating toll plaza events are written in `java`. It generates toll events and push these to a `mysql` database. The `mysql` database was set up on the Linux box described above. `phpMyAdmin`, an administration tool for `mysql` was set up along with `Apache`.

The setup was performed as indicated below.

```
apt-get install apache2
```

PHP5 was installed and `Apache` restarted.

```
sudo apt-get install php5 libapache2-mod-php5
sudo service apache2 restart
```

The installation of `Apache` and PHP5 was verified by creating a test page, `test.php`, under `/var/www`, with the following code.

```
<?php phpinfo(); ?>
```

The setup was verified by running `test.php` in a web browser.

```
http://localhost/test.php
```

`mysql` was set up issuing the following command.

```
sudo apt-get install mysql-server
```

Opening `/etc/mysql/my.cnf` The `bind-address` was changed from `127.0.0.1` to `0.0.0.0`, making it listen on all interfaces.

Next the `root` user was set up with a password.

```
mysql -u root
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('
password');
```

After the `root` user was set up, a database was set up for this project along with a user.

```
mysql> CREATE DATABASE masterdb;
mysql> GRANT ALL PRIVILEGES ON masterdb.* TO 'master_user
'@'%' IDENTIFIED BY 'password';
```

phpMyAdmin was set up with Apache.

```
sudo apt-get install libapache2-mod-auth-mysql php5-mysql
phpmyadmin
sudo service apache2 restart
```

### 3.3.3 mySQL setup

A database was set up on the mySQL server. The table was named `AutoPASS`. Listing 3.1 shows the SQL syntax. An index was created on the timestamps as an effort to speed up queries where a specific time interval was queried. This makes *WHERE* clauses on timestamps faster as mySQL does not have to sequentially search through the whole dataset. There is no 'free lunch' and maintaining the B-tree of indexes make inserts more costly.

```
CREATE TABLE AutoPASS (
    id INT AUTO_INCREMENT NOT NULL,
    name ENUM('Bjørndalen', 'Klett 707', 'Klett E6', '
        Kroppan Bru', 'Leirfossen', 'Sluppen Bru', 'Være
        ') NOT NULL,
    timestamp BIGINT(14) UNSIGNED NOT NULL,
    heavyVehicle BOOLEAN NOT NULL,
    price FLOAT(6,2),
    hasTag BOOLEAN NOT NULL,
    OCRsuccess BOOLEAN NOT NULL,
    PRIMARY KEY (id)
);

CREATE INDEX time
ON AutoPASS (timestamp);
```

**Listing 3.1:** SQL syntax for the AutoPASS table

### 3.3.4 Java

Figure 3.4 shows a rough design of the system to be implemented. The `Generator` class contains functionality to create toll passages based on the methodology outlined in previous sections. The transactions are pushed to an `SQLWorker` that will push the data into a mySQL database. Graphs are generated in the `Graphing` class by reading the data back from the database. General statistics, for example number of



transactions and total amount of money collected, are generated in the `Statistics` class. The `GUI` class displays the graphs and statistics.

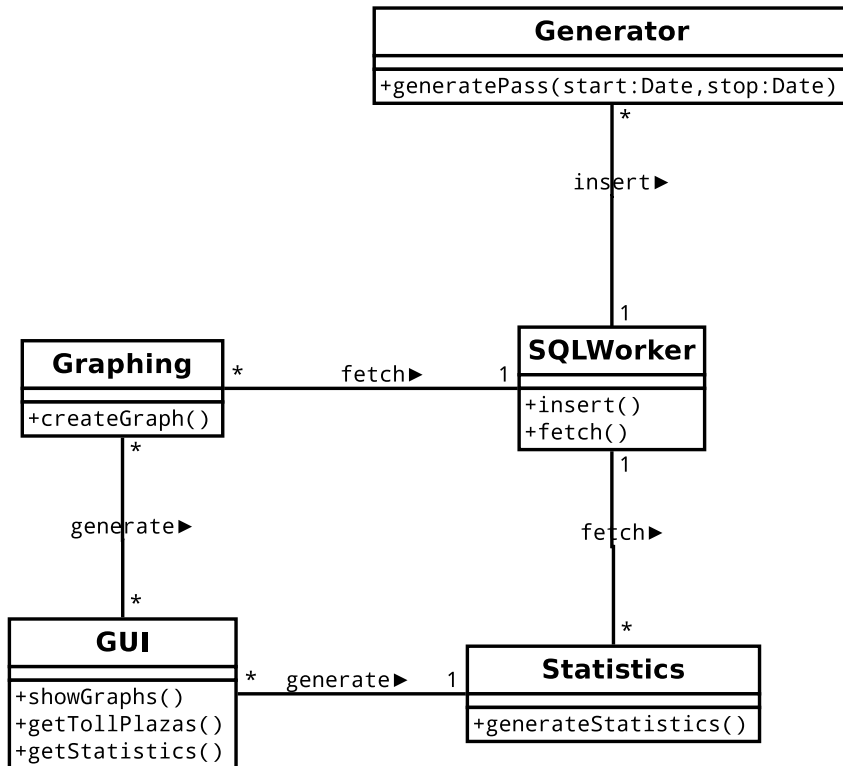


Figure 3.4: Class diagram

The following external libraries were used in the process. **JFreeChart** is a graphing library for the Java platform. **JCommon** is a dependency used by **JFreeChart** that provide layout, configuration and interface classes. For more information on the **JFree** project, the reader is directed to <http://jfree.org/>. The **mysql-connector** is a driver that allows you to connect to a **mySQL** resource in **java**. For more information the reader is directed to <http://dev.mysql.com/downloads/connector/j/>.

<code>jfreechart-1.0.14</code>	Graphics tool
<code>jcommon-1.0.17.jar</code>	Dependency for <code>jfreechart</code>
<code>mysql-connector-java-5.1.24-bin</code>	Handles connection to <b>mySQL</b> database

**Table 3.4:** Java included libraries

# Chapter 4

## Results

### 4.1 Simulation

As a test case the `Java` simulator has been used to generate three months of test data. Data from 1<sup>st</sup> January 2013 until 31<sup>st</sup> March 2013. That amounts to over 11 million transactions stored in the database. It turned out rather quickly that the limited hardware on the Linux box was not optimal for such a large amount of inserts. The hard drive got saturated with writes right off the start. Some efforts were made to optimize the `mysql` settings - increasing buffer pool sizes and flush methods. Norwegian University of Science and Technology (NTNU) also provide a `mysql` database for students\*. This setup outperformed the local database running with optimizations, comparing inserts per second.

For this test the NTNU database was used without any changes to the default settings. Generating and writing the whole dataset was timed, and the process took 182 minutes. Looking into the space usage provided the following statistics. The data in the database amount to 455.9 MiB. The indexes on the primary key and timestamp account for 329.0 MiB, making the total storage space 784.9 MiB. This is summarized in table 4.1.

---

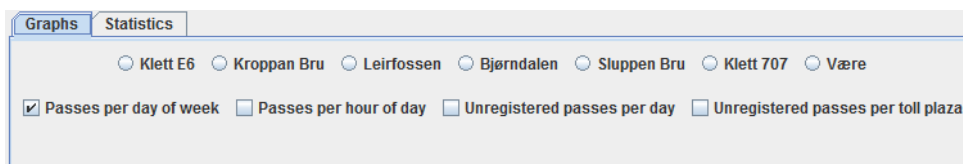
\* [mysql.stud.ntnu.no](http://mysql.stud.ntnu.no)

Generation time	182 minutes
Storage space	784.9 MiB
Entries	11 200 000

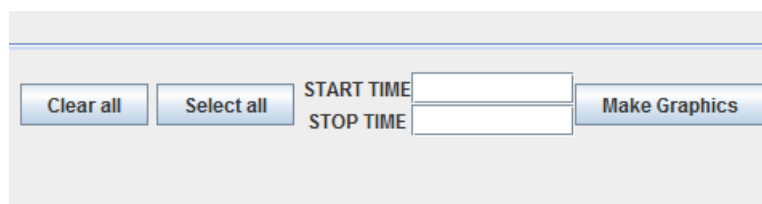
**Table 4.1:** Database parameters

## 4.2 Program for displaying the statistics

This section concerns the program developed to display the statistics made in the simulation. The program has two tabbed panes where one can select either graphs or statistics. Figure 4.1 and 4.2 shows two excerpts of the graphics pane. Four types of graphs can be generated, weekly transactions, daily transactions, daily unregistered transactions, and unregistered transactions per toll plaza. For every graph one can select which toll plazas to include transactions from by checking the radio buttons. Two buttons are provided to set all and clear the selected toll plazas respectively. The wanted time interval is entered into the `start`- and `stop` time boxes. The time must be formatted as `yyyyMMddHHmmss`, where `y` is the year, `M` is the month, `d` is the day, `H` is the hour, `m` is the minute, and `s` is seconds. `20130101000021` means Tuesday 1<sup>st</sup> 2013 00:00:21. The time interval is used to format an SQL query to fetch the transactions within the given time interval. Pressing the make button generates the graph indicated in the check box group.



**Figure 4.1:** Screenshot of graphics pane showing toll plazas and graphing options



**Figure 4.2:** Screenshot of graphics pane showing time fields and make button

### 4.2.1 Database statistics

Figure 4.3 shows a view of the data stored in the database. The shown parameters include the number of stored transactions, the number of transactions where the vehicle could not be identified, the percentage of vehicles above 3.5 tonnes, the date for the first and last entry in the database, and the total amount of money charged. In this run there were 11 200 000 transactions in the database. 42051 of these were

transactions where no money could be charged, meaning that the vehicle had no OBU or the transaction failed, the OCR function could not find the license plate, and the manual inspection was not successful. The percentage of heavy vehicles is 18.62 percent. The date for the first and last record on file is Tuesday 1<sup>st</sup> January 00:00:01 CET 2013 and Saturday 30<sup>th</sup> March 20:00:00 CET 2013 respectively. The total amount of money collected is 98 132 202 NOK.

We see that the number of no-charge transactions match the probability of not being charged calculated in equation 3.3

$$P_{\text{no charge}} = \prod_{i=1}^3 (1 - P_i) = (1 - 0.85) \cdot (1 - 0.95) \cdot (1 - 0.5) = 0.00375 \quad (3.3)$$

$$P_{\text{observed}} = \frac{42051}{11200000} \approx 0.003754 \quad (4.1)$$

#### 4.2.2 Transactions per day-of-week

Figure 4.4 shows transactions per day of the week for all the toll plazas combined. We see the week spanning from 1<sup>st</sup> to 7<sup>th</sup> of January 2013. Wednesday, Thursday, and Friday were the days in the week with the highest number of transactions - all peaking with over 140 000 transactions per day. The transaction count on Saturday and Sunday are approximately 97000 and 87000 respectively.

#### 4.2.3 Transactions per hour-of-day

Figure 4.5 shows transactions per hour of the day for all the toll plazas combined. The underlying distribution is as shown in figure 3.1 on page 34. Looking at the traffic pattern, it increases as people travel to work, decreases after that and increase as people are going back home. The graph shows that on the given day, 1<sup>st</sup> of January 2013, the traffic in all toll plazas combined was at its highest between the hours of 15 and 16, peaking at just above 11000 cars in that hour ( $\approx 183$  cars every minute).

#### 4.2.4 Unregistered transactions per day

Figure 4.6 shows transactions where no vehicle was charged and displays it per day of the month. In this example all toll plazas were selected, so the resulting graph is an aggregate of unregistered passes recorded at every toll plaza. Looking at the figure we see that the 23<sup>rd</sup> of the month stands out with a sum of over 580 unregistered passes.

### 4.2.5 Unregistered transactions per toll plaza

Figure 4.7 shows unregistered transactions per toll plaza in a cake diagram. The figure shows that the highest number of unregistered transactions are recorded at Kroppan Bru, with 23 711 unregistered vehicles from 2013-01-01 to 2013-03-31.

## 4.3 Evaluation of data

All the data used to make the graphics are simulated and not real. One observation with the use of such data is that when looking at the big picture, for example the total number of cars, total number of unregistered cars, total percentage of heavy vehicles, total amount of collected money, the figures might seem reasonable. What such a model often fail to capture however, is the smaller nuances and the seemingly smaller 'events of randomness' one might find in the real world. Examples could be traffic accidents, weather conditions, or even equipment malfunction to some extent. Traffic accidents may impact the graphs in many ways; the peaks in traffic might be shifted, or flattened. A traffic accident near one toll plaza might cause the traffic to be redirected onto another road and subsequently another toll plaza.

Figures 4.4 and 4.6 show the number of passages per day of week and the unregistered passages per day of the month respectively. The two graphs are correlated in the respect that we see more unregistered passes on the days where the traffic is higher. This result is expected based on the simulated probabilities and the expected values. The graphs show that the collections of toll plazas at Kroppan Bru see the most traffic, as shown in figure 4.7, with over 50 percent of the overall traffic recorded in the simulation.

Figure 4.3 show that there are 42 051 vehicles that could not be identified over a timespan from 2013-01-01 to 2013-03-31. Compared to the total transactions on record this amounts to  $\approx 0.375\%$  of the total number of transactions. This does not seem like a big number, but let's put it into perspective. The total amount of charged money amounts to 98 132 202 NOK. Divided out over every transaction that was charged this gives a sum of 8.79 NOK per passage on average.

$$\frac{98132202}{11200000 - 42051} \approx 8.79 \text{ NOK/passage} \quad (4.2)$$

Taking into consideration the 42 051 vehicles that were not charged and multiplying in the average rate gives a total lost revenue of **369 831 NOK**. This is an optimistic estimate based on the number of users with special contracts and rebated fares. It is assuming that all transactions, where an AutoPASS tag is registered, are entitled to a rebate (excluding the toll plaza at Kroppan Bru where no rebate is given). In

reality the average rate will probably be higher. As an example, an increase of the average price per pass by 10 percent increases the lost revenue to  $\approx 407\,000$  NOK.

### 4.3.1 Example of a specific case

Figure 4.8 shows a set of images captured from the simulation program. The figure shows a peak in unregistered passages at Kroppan Bru for that day with just over 332 entries.

Looking at the graph showing the breakdown in unregistered passes for the whole month, this toll plaza show more or less consistent pattern for high number of unregistered transactions for the last three days of the week, Friday, Thursday, and Wednesday (Dates 8, 7, 6, 15, 14, 13, etc.). If such consistent patterns are observed in a real life scenario it is a strong indicator to the fact that this toll plaza should be prioritized. If, however, only single peaks show up, the decision on when to put up controls are not that simple to make. It is interesting to check if such single peaks can be correlated with local conditions. Say for example that in a period with a heavy snowfall there is especially one toll plaza that shows an increased number of unregistered passages, or on cold, dry days where the usage of studded winter tires contribute to an increased amount of dust particles in the air. This knowledge can also be valuable in a situation where one needs to prioritize between plazas.

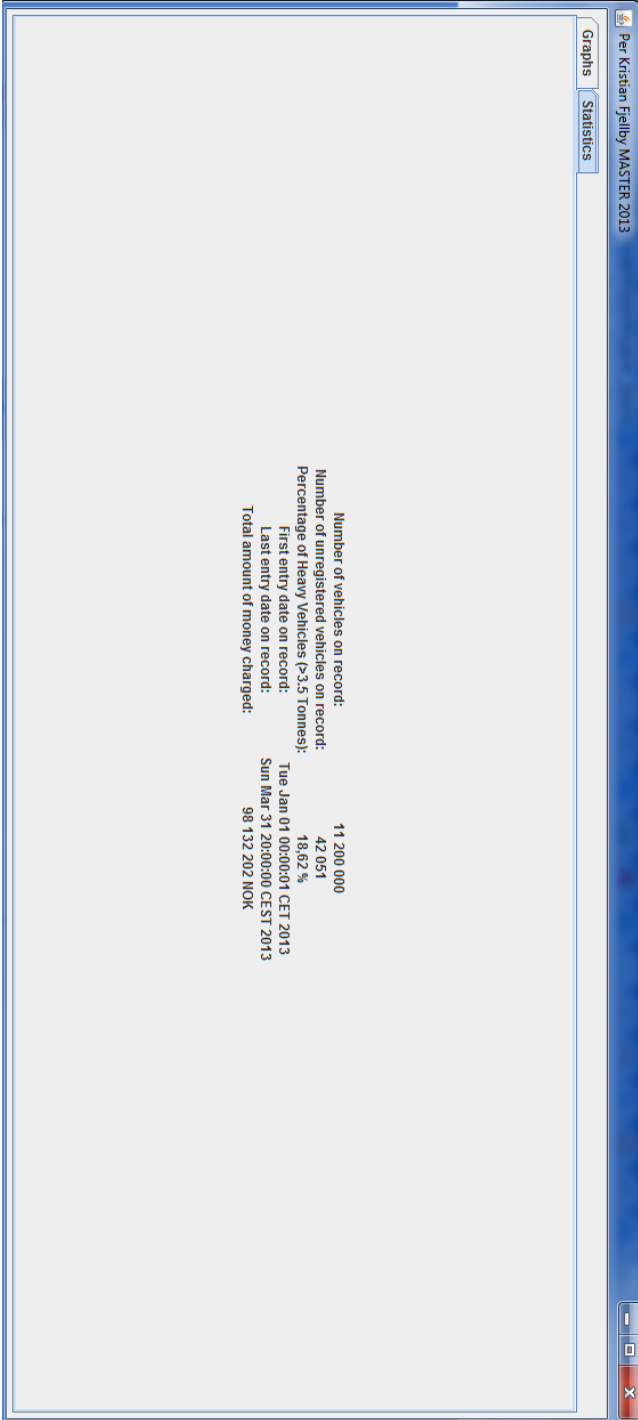


Figure 4.3: Database statistics shown through Java



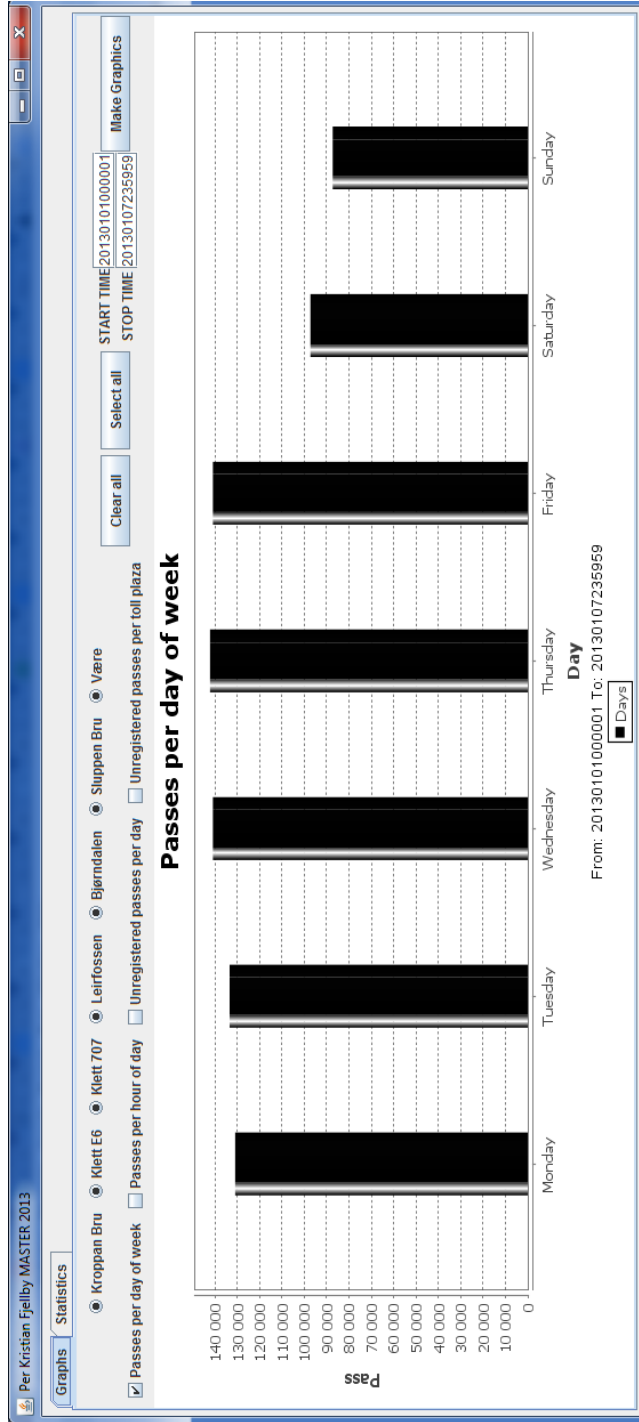


Figure 4.4: Registered transactions shown per day of week

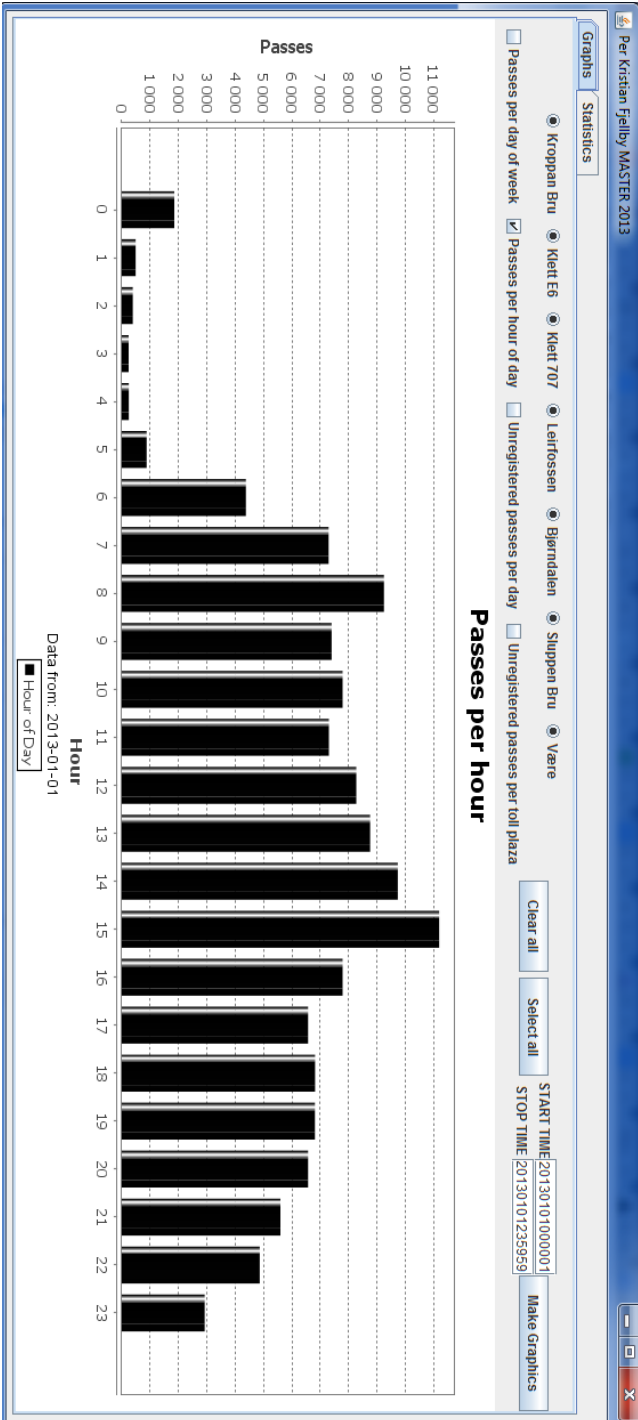


Figure 4.5: Registered transactions shown per hour of the day

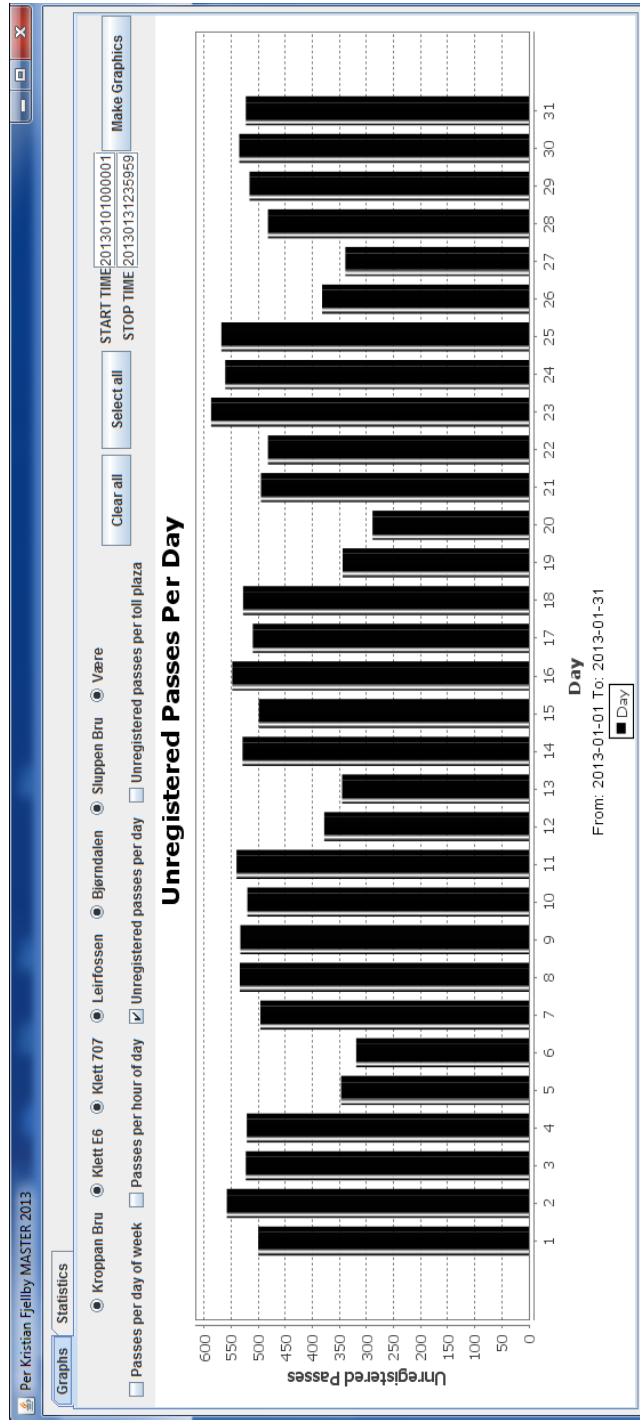


Figure 4.6: Unregistered transactions shown per day of month

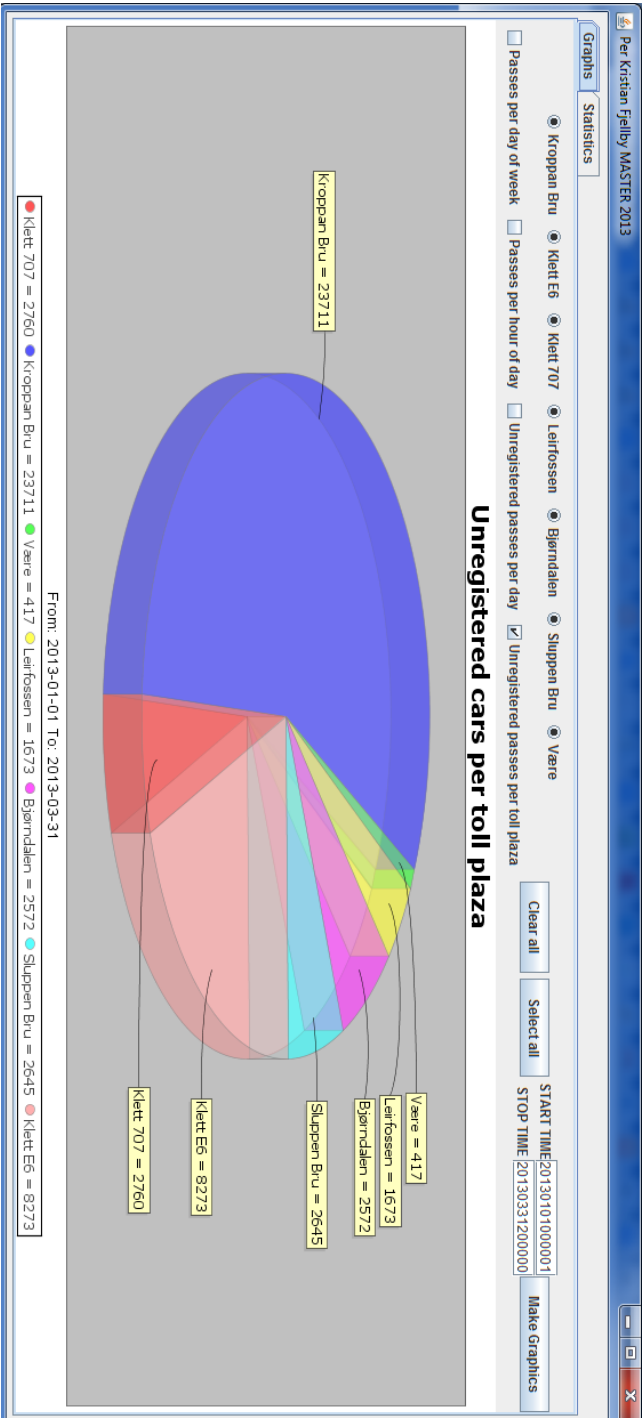


Figure 4.7: Unregistered transactions shown per toll plaza

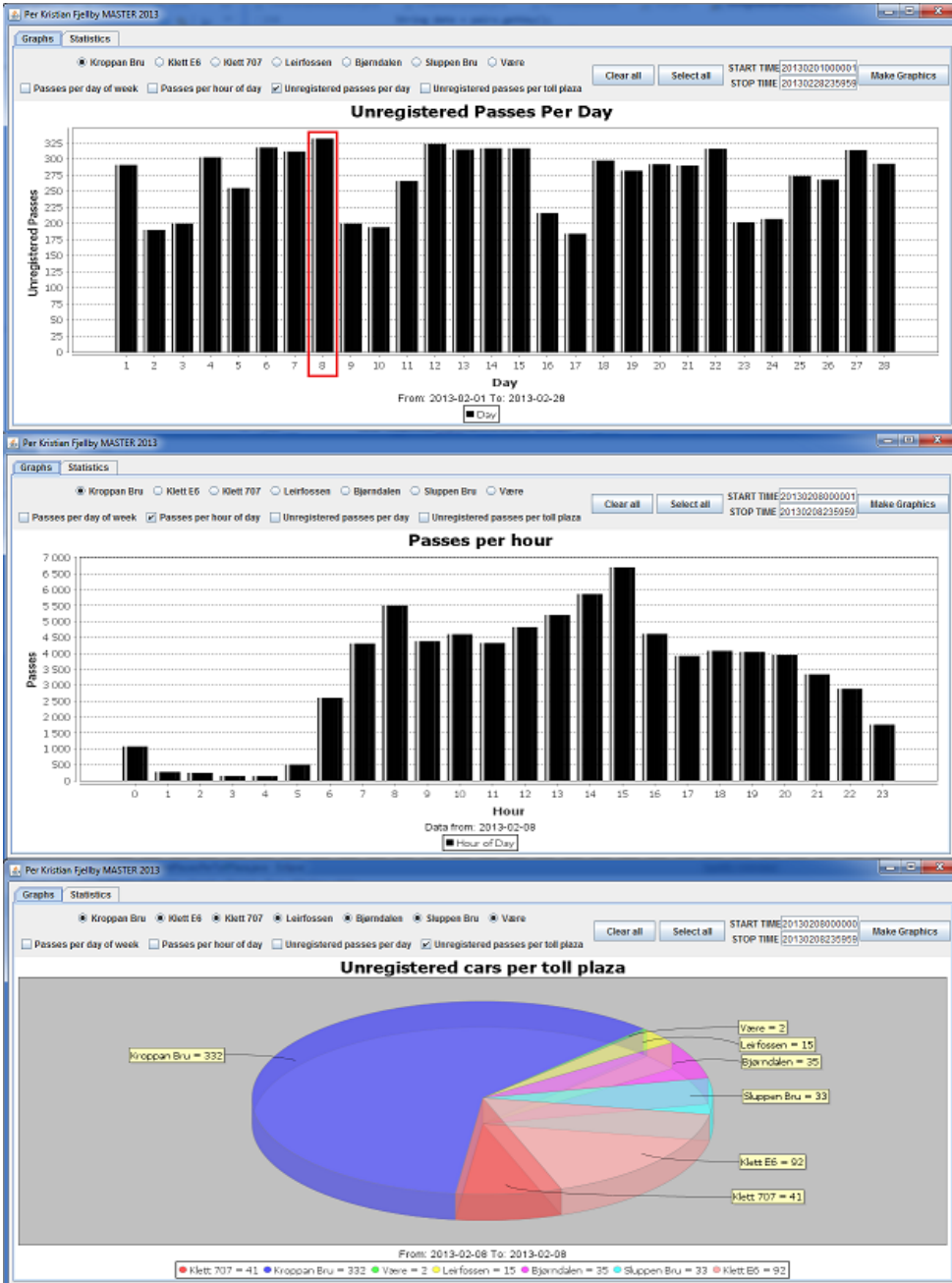


Figure 4.8: Collection of figures showing a peak in unregistered passes at Kroppan Bru on 8<sup>th</sup> February 2013



# Chapter 5

## Discussion

### 5.1 Simulation

What we set out to test was if it is possible to use anonymous traffic statistics to assist in the process of identifying cars that are not charged. The analysis of traffic data can reveal patterns that can direct the toll companies and their efforts for overcoming the problem. Storing vast amounts of data that are directly linkable back to concrete individuals, for a longer period of time than necessary for providing the toll road service, is not desirable. The following section gives an overview of the data the system is built upon.

#### 5.1.1 Anonymization

For a dataset to be characterized as anonymous there should be no way of linking the information to an individual person. As an example, the license plate number and OBU id are pieces of information that can be directly tied to an individual. The license plate number can be cross-referenced with the vehicle register to reveal the owner; the OBU id can be checked against a list of active AutoPASS subscriptions and reveal the owner of the account. Both are examples of parameters that should be avoided.

The data that are stored for a given transaction in the simulator is listed in table 5.1.

None of the parameters can be used to directly tie an individual to a passage.

name	Name of the toll plaza
timestamp	Time of the transaction
heavyVehicle	Indicates if the vehicle is over 3.5 tonnes
price	The price charged for the transaction
hasTag	Indicates if the AutoPASS transaction was successful
OCRsuccess	Indicates if the OCR function was successful, either automatically or by manual inspection

**Table 5.1:** Parameters that are stored in the database

### 5.1.2 Executing a control

If a toll station is selected for control a new set of problems arise. Inspectors need to be warned when a vehicle passes the toll plaza unidentified. Unidentified in this sense means a car that does not have a working AutoPASS tag and the OCR check is negative. In the real system, if no tag is present and the OCR fails, the manual inspection of the photographs is the last instance for identifying the vehicle. At this point one does not know if the photographs will reveal the license plate number by manual inspection. To make the control as efficient as possible, only vehicles that fall into the category which are not identifiable by manual inspection should be stopped. This means that operators have to inspect the photographs and make their decision in real time. A setup that displays the front- and rear view of the license plates of these flagged vehicles will simplify the work process. The operator then assess if identification is possible or not. In the latter case the car should be stopped. In the former case the car should be allowed to pass and the exception handling of that passage should be carried out as in the normal case.

Figure 5.1 shows one of the toll plazas located near Kroppan Bru in Trondheim. The setup of an efficient control point could prove difficult. You want to disrupt the normal traffic as little as possible and at the same time have a safe area to stop cars for control in the near vicinity of the toll plaza. Monitor stations would typically be located near to the road side equipment, both for ease of access to the data from AutoPASS, but also easier visual identification of the vehicle to be stopped - an accurate description of the vehicle in question can then be radioed to the officers at the control point.





**Figure 5.1:** Toll Plaza near Kroppan Bru. Not necessarily room for stopping cars. Image attribution: *Google Maps* [19]

### 5.1.3 Legal issues

It makes sense to mention some legal issues related to stopping cars in the way described in previous sections. Considering who should carry out the controls is an important question. Looking to other areas of public transportation and using buses as an example, passengers using the service have to accept the transport regulations set forth by the company. As a concrete example, if one travels by one of AtB's buses in Trondheim, the company's transport regulations give the driver and separate inspectors the right to control your travel documents [4, §7]. Travelers who at the time of control cannot provide proof of valid travel documents are issued a fine. Adopting this scheme to the toll road sector is an interesting thought, but is not necessarily a straightforward adoption. The cars that should be stopped all have discrepancies related to the license plate, but they may need to be handled differently with respect to the law. Not drawing any conclusions to how the laws are to be interpreted, there is a difference in stopping a muddy car with unreadable license plates and stopping a car with no license plates at all. Not to mention if the control reveal deliberate efforts where the license plates are obscured to avoid paying toll. The latter is probably a good reason to press charges. Nonetheless, a review of the technical state, especially related to the visibility of license plates, is

best left to representatives of the NPRA or the police, likewise is issuing tickets for law violations also a police matter. As a minimum, the stopped car should be charged for the passage. In regard to the other violations mentioned above it should be up to law enforcement officers to assess further action. An important factor is the general deterrence aspect - if the public see that focus is given to this area and that deliberate efforts to avoid paying toll is not accepted, it can deter others from attempting the same. The increased possibility of being caught might contribute positively in this sense.

#### 5.1.4 Related systems

A system that is operating in a similar area as the one outlined in this report, is the system used for automatic number plate recognition by the NPRA. The system is used to sort out cars that have prohibitions, no insurance, are stolen, or any other reason, based on the NPRA's registers, for not being on the road. The system takes a photo of the license plate of the vehicle, use OCR technology to recover the license plate number, and cross-reference the number against a list of vehicles with prohibitions. This gives more efficient controls, as only vehicles with registered prohibitions are stopped. The Norwegian Data Protection Authority (NDPA) has issued a report regarding an inspection they conducted of the system and the NPRA 17.08.2012 [6]. This report is relevant with respect to the control situation outlined for unregistered passages in the AutoPASS system, but also in the context of gathering statistics.

Regarding the latter, the NDPA observes that statistics are generated for the purpose of allocating resources at times when they can be best utilized [6, p. 3]. This is an argument which is in agreement with the proposed scheme for AutoPASS outlined above. The license plate numbers that trigger an alarm are stored for one hour before they are deleted. This is the case for both the roadside control situation as well as the in the case of statistics generation. License plate numbers that do not trigger an alarm are immediately deleted in the roadside control situation. In case of generating the statistics for these passes, the event is registered and then deleted. An important aspect is that the NDPA finds that the generation of statistics involves personal information and thus should be handled in accordance with the Personal Data Act. With the Personal Data Act as a foundation, the question becomes a trade-off between the NPRA's interest in the information and an individual's right to privacy - this is also an issue covered in the law, where the right to handle personal information can exceed the right to individual privacy if the reasons for storing the information are found to be of greater importance than the right to privacy [24, §8f]. What justifies as important reasons in this matter is not easily answered. To avoid this issue in an AutoPASS setting, the stored data, for the purpose of generating statistics, need to be anonymized in a timely and sufficient way so that

the information can be handled on a general basis that is not governed under the Personal Data Act. Looking closer at the control situation, the vehicles that are stopped have triggered an alarm based on the license plate number. In the event of an alarm, a number of parameters are collected from other systems. Some examples include: the reason for the flagging of the license plate, color of the license plate, color of the vehicle, the date the vehicle was flagged, the date the vehicle was registered in Norway, vehicle group, and brand. In addition, the persons in the vehicle can be identified as a result of the control.

The NDPA concludes that, pursuant to the law, the NPRA can handle personal information for the purpose of inspecting vehicles [6, 7.2.3]. At the same time, the NPRA is ordered to stop handling personal information for the purpose of generating statistics, *or limit the handling to a minimum required for generating statistics and subsequent deletion of the data as soon as the statistics are generated* [5].

The lessons that can be learned from this project, and related to the AutoPASS sector, are that the purpose for generating statistics need to be well founded and organized, even more so if handling personal data is involved. The NDPA enforce strict guidelines when it comes to how long time one can store personal data - given the previous example, the sooner the data is deleted the better. The foundation for using electronic aids in relation to traffic controls looks to have been given the green light. The argument of aiding in the purpose of controlling vehicles is also transferable to the AutoPASS scheme, as the main purpose of the control is to identify the discrepancies regarding unreadable license plates.

## 5.2 Anonymity

### 5.2.1 Anonymity in AutoPASS

The first part of this section will cover the pieces of information that are stored in the AutoPASS system. As previously mentioned you need to enter into a contract with an issuer who will then provide you with an AutoPASS tag. As an example, if you want to enter into a contract with Fjellinjen you are required to provide the following information: First- and last name, address and postcode, country, e-mail telephone, date of birth, bank account number, vehicle license plate number, vehicle brand, contract start date, vehicle class, and vehicle nationality. A photocopy of this contract can be found in appendix C. This information is stored along with your AutoPASS tag number and central account details.

The NDPA has regulated the electronic toll sector. If a company wants to operate a

fully automatic toll plaza and store personal information they need to apply for that privilege. The NDPA sets a number of requirements for granting the application. One requirement is to implement an *'alternative payment solution'*. The complete set of requirements can be found in [13]. Personvernemnda is a body of appeal under the NDPA. The NDPA decided to regulate the electronic toll sector in February 2005 - the decision was appealed by the NPRA [31]. One point of dispute was that manual toll plazas allowed the users to travel the roads more or less anonymously - an introduction of the AutoPASS system would not provide the same level of privacy for the users. The NDPA pushed for a system that ensured the user's right to privacy. Discussions went back and forth [31], and Personvernemnda was required to decide what requirements the regulation should impose on the operators.

The first alternative that was assessed was an anonymous AutoPASS tag where the tag can exist without being registered with a specific user. Right of the bat this solution seems to provide a better approach to the anonymity issues as the link between the user and tag is removed. From the viewpoint of AutoPASS, if the transaction is successful and the correct amount of money is deducted from an account, who owns the account should not really matter. This is also the rationale behind the alternative. Money is prepaid into an account and used as in the normal use case. However, the initial deposit should probably be paid out in cash to avoid any credit card transactions being linked with the tag. Another problem arises when the balance of the tag is approaching zero. Since the toll company does not know who you are they cannot send you an invoice or reminder to deposit more money. The only indication the user gets is the light signal at the toll plaza indicating that the balance is low. Continued use of the tag without depositing more money will trigger video identification, which effectively abolishes any anonymity.

The second alternative is to enter into an AutoPASS contract as normal, but the company provides an alternative subscription where transaction logs are deleted as soon as possible. [31] states the requirements for such subscriptions. An excerpt of the requirements that relate to *when* data have to be deleted is included below.

- Storage time for transaction data at the toll plazas shall not exceed 72 hours.
- Processing time in the central system, and subsequent deletion of the transaction, shall not exceed 1 hour in the normal case. Transactions from other operators' toll plazas need to be processed and deleted within 24 hours.

In appendix C the point in the contract where you can chose this alternative subscription is highlighted. In reality this alternative cannot be classified as anonymous - it is just an ordinary AutoPASS contract where the storage time of personal information is limited to a minimum. One of the drawbacks with this alternative (as well as the

previous) is that the ability to dispute transactions is limited. The fact that the operator deletes the transaction from their system makes it fairly easy to state that this is a *'use at your own risk'* offer. Not diving into the legal issues it is however interesting to notice that *Bokføringsforskriften* states that a sales document should contain *time and place for delivery* [22, §5.1.1.4]. The same law also states that documentation should be stored for 10 years. It is obvious that the toll companies have to keep some form of information on the transaction to satisfy the tax authorities. So what is initially stated as being deleted is presumably retrievable within the 10 year limit. The second alternative cannot be described as an anonymous alternative.

Personvernemnda, who were to decide in this matter, ended up choosing the latter alternative. The right of the NDPA to regulate the sector was upheld, alternative two was assumed as the foundation for the regulation with the time limits mentioned above. In addition, the NPRA was instructed to conduct an annual audit of the toll companies to check that these requirements were met [31].

The fact is that the current system provides little to no anonymity. The problem seems to be that the system 'allow' users to travel through AutoPASS lanes without paying - the cameras are needed to be able to go back and identify transactions that were not valid. The photography and subsequent identification of the vehicle is troublesome no matter how you relate it to anonymity. Even if good routines for deletion together with audit procedures intended to enforce these deletion routines are created, people concerned about their anonymity will probably still show skepticism toward the system. Undeleted data is always a subpoena away or perhaps a law enforcement agency will subpoena a company to not delete future transactions in the interest of aiding an investigation. To increase the anonymity, the link between AutoPASS tag and personal information must be removed. In a digitalized society this is surely a daunting task. The financial system is built up in such a way that making anonymous payments is hard. AutoPASS is a system where money changes hands and complete anonymity is thus hard. About the only way to exchange money without a digital record is through cash payment, provided that the transaction is carried out without any personal information being shared. This was an alternative when the toll roads were equipped with manual lanes accepting cash payment. This alternative was effectively abolished with the free-flow, non-stop plazas we see today. One very good reason why transferring money anonymously should be hard is to fight crime or restrict the flow of money related to criminal activity. This has more or less become a norm in society - we accept that our digital transactions are subject to audit by governmental institutions where one of the benefits is that it becomes significantly harder for criminals to move money.

### 5.2.2 How is anonymity handled in other countries

An interesting question is to look to other countries to see how they handle the same issues of user anonymity. The toll charging on the Golden Gate Bridge in San Francisco has an option they market as anonymous [12]. The setup looks quite similar to the first alternative discussed in the sections above. You can open up a **FasTrak** account, which is what the system is called, where you are not required to provide any personal information. Money is deposited in form of a cash payment. When the toll balance is low you have to show up at a customer service center and refill the account. If the account is not refilled and still used an invoice will be mailed to the owner of the vehicle.

The 407 ETR in the province of Ontario, Canada provides users with a payment option marketed as an anonymous account. The user is provided with a tag without registering any personal information. Money is deposited by cash with an initial deposit of \$57.20 per transponder and an initial payment of \$200.00 in prepaid funds. Anonymity is lost if the credit balance falls below \$0.00, if the transponder malfunctions, is damaged in any way, not installed properly, or is lost or stolen. The anonymous account is only available to cars with a GVWR under 5000 kg. The terms also state that anonymity is lost if required by law pursuant to a criminal investigation. There is no guarantee that there will not be taken a video image of a vehicle with an anonymous tag. The terms can be found in [1].

### 5.2.3 A step toward bettering the anonymity in AutoPASS

Over the course of the last sections we have identified some key issues with today's system. For AutoPASS to provide something which can be classified as an anonymous toll payment scheme some improvements are needed. An initial observation is that it would be hard to keep a post-payment scheme where you are billed after the passage - the toll road company would not be able to identify the user. Some efforts have been put into schemes using blind signatures, zero-knowledge proofs, and digital signatures. One such effort is outlined in paper [20]. They propose a post-payment scheme they claim will give the user anonymity, in the sense that the trips are not reconstructable, and guarantee the toll operator will receive the charges for all trips made by a user [20]. The rationale is sought outlined below with the use of RSA blinding. An introduction to RSA and blinding signatures are given in appendix D.

A **Motorist** and a **Toll company** enter into a contract regarding the usage of toll roads. The **Motorist** is provided with a transponder which is equipped with a set of digital identities  $D = \{id_1, id_2, \dots, id_n\}$ . These identities should not be known to the **Toll company**. The **Motorist** blinds the identities and sends them to the toll

company

$$D_{\text{blinded}} = \{id_1 \cdot r^e \bmod n, id_2 \cdot r^e \bmod n, \dots, id_n \cdot r^e \bmod n\} \quad (5.1)$$

The article then states that the **Motorist** should provide the **Toll company** with a digital signature of the list of identities to avoid repudiation. The **Motorist** digitally signs the set of identities and provides the **Toll company** with the signature. These digital identities should be unique, so the number of possible identities needs to be large to make the probability of choosing equal identities small.

The **Toll company** signs the blinded signatures and return them to the **Motorist**

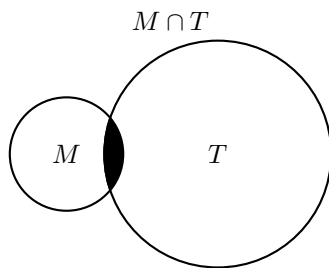
$$D_{\text{signed,blinded}} = \{(id_1 \cdot r^e)^d \bmod n, (id_2 \cdot r^e)^d \bmod n, \dots, (id_n \cdot r^e)^d \bmod n\} \quad (5.2)$$

The **Motorist** is now equipped with a set of identities which he will use at the toll plaza. There is a distinction between *open* and *closed* tolling systems. In the former system the **Motorist** uses a fresh *id*. After it is used, the *id* is stored in a list of used *ids*. In the latter type of system the charge is dependent upon the entry- and parting toll plaza. For the system to be able to calculate the correct charge, the same identity has to be provided at point of entry and point of departure. When a **Motorist** enter into a closed tolling system he is informed that the same identity has to be provided at the departing toll plaza. The *id* is therefore kept available until the **Motorist** has departed. After departure, the *id* is stored in the list of used *ids*.

When the **Motorist** passes through the **Toll plaza**, the **Motorist** is provided with a certificate showing that the **Toll plaza** is signed by the **Toll company** with the purpose of collecting toll. If the certificate proves valid, the **Motorist** provides the **Toll plaza** with an identity  $id_i$  and the corresponding identity which has been blinded and signed by the **Toll company**. The **Toll plaza** can then, with the knowledge of the **Toll plaza's** public key, verify the identity.

If this was an open system, the **Motorist** uses the same *id* when exiting the toll road. The **Toll plaza** sees that the same *id* has been used both inbound and outbound and is able to calculate the correct toll charge. The *id*, along with the calculated charge is sent to the **Toll company** and stored in a list of receivables. The **Motorist** also stores the *id* in a list holding all the used *ids*.

The **Motorist** is responsible the *ids* that make up the intersection between M and T shown in figure 5.2. This is the intersection between the **Motorist's** *ids* and the *ids* stored by the **Toll company** for charging. The **Motorist** and **Toll company** now enter into a reconciliation protocol where the *ids* in the intersection are billed the



**Figure 5.2:** Intersection between the Motorist's (M) used *ids* and the Toll company's (T) stored *ids*.

**Motorist.** The **Motorist** calculates the intersection between the receivables-list from the Toll company and his own used-*ids* list. A zero-knowledge proof is made by the **Motorist** to the fact that all identities are accounted for. The result is sent to the Toll company which generates an invoice, without knowing the digital identity (just the digital signature) of the **Motorist**. The **Motorist** cannot cheat as he signs the blinded identities and must prove that all *ids* are accounted for in the reconciliation process.

#### 5.2.4 Evaluation of the protocol

The proposal given in [20] represents an effort to utilize cryptographic principles to a much larger extent compared to previously outlined anonymous AutoPASS alternatives and the examples from San Francisco and Toronto. The original paper does not give any concrete implementation of the proposed protocol, for example how the blind signatures are made, how the lists are shared, or how the zero-knowledge proof is accomplished. The introduction of blinded RSA signatures in the outline given above represents a small, yet important, contribution in this respect. If such protocols are to become a reality, they need to be laid out explicitly, with full description of the underlying cryptographic mechanisms.

The proposed protocol differs from other anonymous toll protocols in the way of post-payments. In both examples given earlier, the user is required to make payments in advance, and loses anonymity if the tag is used with insufficient credit balance. Post-payments shifts a lot of responsibility over on the users - in the outlined protocol, if users fail to participate in the reconciliation protocol, the toll company is not able to identify them. If the used *ids* of the motorist are stored on the OBU and it is suddenly lost, intentionally or unintentionally, the reconciliation protocol does not work. For a motorist to not partake in the reconciliation phase is unacceptable to



the toll company, so there need to be sanctions for intentionally failing to prepare the OBU for reconciliation. On the other hand, malfunction or failures of the OBU where the owner is not to blame, poses a risk for the tolling company, as potential revenue is lost.



# Chapter 6

## Conclusion and further work

### 6.1 Conclusion

This thesis has provided an introduction to the AutoPASS system currently used on toll roads in Norway to provide a free-flow, non-stop payment service for levying toll. As a contribution to help solve the problem with a high number of unidentified passages, a simulator and analysis tool have been set up. The purpose of the simulator was to generate traffic data for the analysis tool to process. The analysis tool is meant to be an aid in the process of directing resources to toll plazas that show the highest number of unregistered passages. By analyzing the output from the program a strategy for executing manual controls can be planned and set up at places where the hit-rate will be large. Results have shown that toll plazas that stand out with respect to the number of unidentified passes can be identified based on statistics that does not reveal personal information about the driver of the vehicle.

The anonymity issues of AutoPASS are addressed and the communication between the NDPA as regulator and the NPRA as owner has been covered. A view of how other countries handle the problem of anonymity is given. Lastly, an initiative to provide a better Electronic Toll Collection (ETC) protocol with respect to anonymity is covered. This shows that there are possibilities to better the situation. The NDPA is an important advocate for the individual's right to privacy, but that alone is not enough. For changes to happen and more focus to be given to anonymity, individual users need to express their concerns and call for better solutions.

## 6.2 Further work

The next step further would be to test the system on real production data. Statistics need to be generated from the central system according to what is outlined. There are still some legal issues that need to be dealt with and lessons can definitely be learned from the automatic number plate reading system used in conjunction with the road traffic controls. The reports referenced in regard to the latter system are of recent date, and the deadline for improvements of the shortcomings revealed by the NDPA in their investigation of the NPRA was 1<sup>th</sup> of June 2013. The development of this case will play an important role and lay much of the foundation that the proposed system for AutoPASS will have to deal with.

# References

- [1] 407ETR. Anonymous Account. <http://www.407etr.com/payments/anonymous-account.html>. Accessed 13. June 2013.
- [2] Adressa.no. *Snart har vi lagt igjen én milliard i bommene*. <http://www.adressa.no/nyheter/trondheim/article7701469.ece>. Accessed 6. June 2013.
- [3] ANPT-tutorial. The automatic number plate recognition tutorial. <http://www.anpr-tutorial.com/>. Accessed 8. June 2013.
- [4] AtB. Transportvedtekter for AtB AS. <https://www.atb.no/transportvedtekter/category487.html>. Accessed 19. June 2013.
- [5] The Norwegian Data Protection Authority. *Statens Vegvesen og Tollvesenet må slette opplysninger fra skiltgjenkjenningssystem*. <http://www.datatilsynet.no/Nyheter/2013/Statens-vegvesen-og-Tollvesenet-ma-slette-opplysninger-fra-sine-skiltgjenkjenningssystemer/>. Accessed 22. June 2013.
- [6] The Norwegian Data Protection Authority. *Statens Vegvesen: Endelig Kontrollrapport*. [http://www.datatilsynet.no/Global/05\\_tilsynsrapporter/2012/12-00753-7\\_Kontrollrapport\\_StatensVegvesen\\_skiltgjenkjenningssystem.pdf](http://www.datatilsynet.no/Global/05_tilsynsrapporter/2012/12-00753-7_Kontrollrapport_StatensVegvesen_skiltgjenkjenningssystem.pdf). Accessed 22. June 2013.
- [7] AutoPASS. AutoPASS Requirement Specification. 4.2 Charging Point Equipment - AutoPASS Radio Link.
- [8] AutoPASS. AutoPASS Requirement Specification. 4.3 Charging Point Equipment - Central system interface.
- [9] AutoPASS. AutoPASS Requirement Specification. 4.4 Charging Point Equipment - Security.
- [10] AutoPASS. Monteringsanvisning for AutoPASS-brikke. [http://www.autopass.no/\\_attachment/71834/binary/369614](http://www.autopass.no/_attachment/71834/binary/369614). Accessed 15. April 2013.
- [11] Trøndelag Bomveiselskap. *Takster for Miljøpakken*. <http://www.trondelagbomveiselskap.no/Takster-979.aspx>. Accessed 26. April 2013.

- [12] Golden Gate Bridge. *I Want to Remain Anonymous*. <http://www.goldengate.org/tolls/iwanttoremainanonymous.php>. Accessed 13. June 2013.
- [13] Datatilsynet. Konesesjon - Helautomatisk bompenggeinnkreving. [http://www.datatilsynet.no/Global/05\\_regelverk/Konesesjoner/autopass\\_konesesjon.pdf](http://www.datatilsynet.no/Global/05_regelverk/Konesesjoner/autopass_konesesjon.pdf). Accessed 12. June 2013.
- [14] Datatilsynet. Oversendelse av klage – Pålegg om konesesjonsplikt for helautomatiske bomstasjoner. [http://www.datatilsynet.no/Global/05\\_personvernnemda/2006/05-152\\_PVN\\_konesesjonsplikt.pdf](http://www.datatilsynet.no/Global/05_personvernnemda/2006/05-152_PVN_konesesjonsplikt.pdf), 2005.
- [15] European Union Commission Decision. 2009/750/EC *Definition of the European Electronic Toll Service and its technical elements*. 2009.
- [16] European Union Directive. Directive 2004/52/EC *Interoperability of electronic road toll system in the Community*. 2004.
- [17] International Organization for Standardization (ISO). *Electronic fee collection - Application interface definition for dedicated short-range communication (ISO 14906:2011)*.
- [18] Trond Foss. Systembeskrivelse. AutoPASS - Samordnet Betaling (ASB). 2003.
- [19] Google. Google StreetView image. <http://goo.gl/maps/5oRwy>. Accessed 18. June 2013.
- [20] Muhammad Usman Iqbal and Samsung Lim. *Anonymous Electronic Toll Collection (ETC)*, 2007.
- [21] L.R. Knudsen and M.J.B. Robshaw. *The Block Cipher Companion*. Information Security and Cryptography. Springer-Verlag Berlin Heidelberg, 2011.
- [22] Norges lover. For 2004-12-01 nr 1558: Forskrift om bokføring. Accessed 12. June 2013.
- [23] Norges lover. Lov 1963-06-21 nr 23: Lov om vegar (Veglova). Accessed 12. June 2013.
- [24] Norges lover. Lov 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven). Accessed 22. June 2013.
- [25] Miljøpakken. Bompunkter. <http://miljopakken.no/om-miljopakken/bomstasjoner>. Accessed 10. April 2013.
- [26] NIST. Federal Information Processing Standards Publication 1981 - Guidelines for Implementing and Using the NBS Data Encryption Standard (FIPS-74).
- [27] Norbit. CEN/TC 278 Microwave OBU for Multi-application DSRC. <http://www.norbit.no/wp-content/uploads/2010/05/databladDesign4raster.pdf>. Accessed 10. April 2013.

- [28] Norvegfinans. Aktører og roller. <http://www.norvegfinans.com/no/bompenger-i-norge/aktorer-og-roller/>. Accessed 20. June 2013.
- [29] SINTEF Teknologi og Samfunn. Informaskinssikkerhet i AutoPASS-brikker. *Sikkerhet i dagens AutoPASS-brikker sett i relasjon til AutoPASS-brikker basert på EN 15509 EFC - Interoperability Application Profile for DSRC*. 2013.
- [30] Marthe Hellum Olaisen. *Personvern hensyn ved innsamling av dynamiske data. Studie av anvendelsesområder for AutoPASS*. Master's thesis, Norwegian University of Science and Technology, 2007.
- [31] Personvernemnda. Klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner. Personvernemndas avgjørelse av 7.3.2006 (..). [http://www.personvernemnda.no/vedtak/2005\\_11.htm](http://www.personvernemnda.no/vedtak/2005_11.htm). Accessed 12. June 2013.
- [32] Riksrevisjonen. *Riksrevisjonens undersøkning av bompengeforvaltninga*. Dokument 3:5 (2012–2013), 2013.
- [33] A. Shamir R.L. Rivest and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 1977.
- [34] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2011.
- [35] European Standard. NS-EN:12253:2004 Road Transport and Traffic Telematics (RTTT) - Dedicated short-range communication - Physical layer using microwave at 5,8 GHz. 2004.
- [36] European Standard. NS-EN:13372:2004 Road Transport and Traffic Telematics (RTTT) - Dedicated short-range communication - Profiles for RTTT applications. 2004.
- [37] European Standard. NS-EN:14816:2005 Road Transport and Traffic Telematics. Automatic vehicle and equipment identification - Numbering and data structure. 2005.
- [38] Statens Vegvesen. Håndbok 146. Traffikkberegninger. 1988.
- [39] Statens Vegvesen. Håndbok 102. Bompengeprosjekter. 2001.
- [40] Statens Vegvesen. Håndbok 281. Veileder i trafikkdata. 2011.





# Appendix

## Doppler shift calculation

Center frequency of the channel: 5.7975 GHz.

$\Delta f$ :  $\pm 1000$  Hz.

If the velocity involved is small relative to the speed of light,  $\Delta f$  can be expressed as

$$\Delta f = \frac{\Delta v}{c} f_0 \quad (\text{A.1})$$

where  $\Delta v$  is the difference in velocity between the two points,  $c$  is the speed of light and  $f_0$  is the emitted frequency.

Rearranging terms gives

$$\Delta v = \frac{\Delta f}{f_0} c \quad (\text{A.2})$$

Inserting numbers gives us the result

$$\Delta v = \frac{1000 \text{ Hz}}{5.7975 \cdot 10^9 \text{ Hz}} 3 \cdot 10^8 \text{ m/s} \approx 51.75 \text{ m/s} \approx 186.3 \text{ km/h} \quad (\text{A.3})$$



# Data Encryption Standard (DES)

DES is a symmetric-key block cipher which started as an IBM project led by Horst Feistel in the late 1960s early 1970s. Feistel and his team proposed an algorithm which was called LUCIFER - a block cipher with 128 bits key size and 64 bit block size. In an effort to commercialize the product on a single chip, the algorithm was modified - one thing that was altered was the key size, which was shrunk to 56 bits\* [34]. When the National Bureau of Standards (NBS), today known as the National Institute of Standards and Technology (NIST), issued a call for a national standard for protecting sensitive information, LUCIFER was submitted in the reduced key size form and was selected as the new data encryption standard. The algorithm is published as standard FIPS PUB 46 - Data Encryption Standard, with later revisions FIPS PUB 46-2 and FIPS PUB 46-3.

LUCIFER, and also DES, is built up around what is known as a *feistel structure*. The cipher works in rounds where data is *substituted* and *permuted*. Substitution means to replace a data element with another, for example to swap the letter 'e' with 'g'. When the cipher permutes the data, nothing is added or taken out, the data is just rearranged to form a new ordering of the data, for example to permute the string 'abcde' to 'badce'. As mentioned this is done in rounds, and in every round, bits from

---

\* Some may say that the key is actually 64 bits, but only 56 bits are used in the cipher, the other eight are parity bits.



**Figure B.1:** DES operations

a key,  $K$ , are put into the mix, successively building up the ciphertext. Decryption is performed by running through the same steps in the inverse order as they were applied. A *round function*,  $F$ , is applied every round, where the substitution and permutation are performed. The input is split into two halves,  $L_x$  and  $R_x$ , where  $x$  designates the round number. The left half,  $L_x$ , is XOR-ed with the output from the round function and passed on as the right input,  $R_{x+1}$ , in the next round.  $R_x$  is used as input to the round function,  $F$ , and used as the left part,  $L_{x+1}$ , in the next round. An overview of the DES round scheme is shown in figure B.2.

## B.1 DES with multiple keys

In order to provide more key-bits and still provide backward compatibility, what is known as triple DES (3DES) in the case of three keys and 2DES in the case of two keys, have been developed. Different versions exist, and they differ in keying options.

### B.1.1 2DES keying

Here we use two independent keys,  $K_1 \neq K_2$ .

$$C = E_{K_2}[E_{K_1}(P)] \tag{B.1}$$

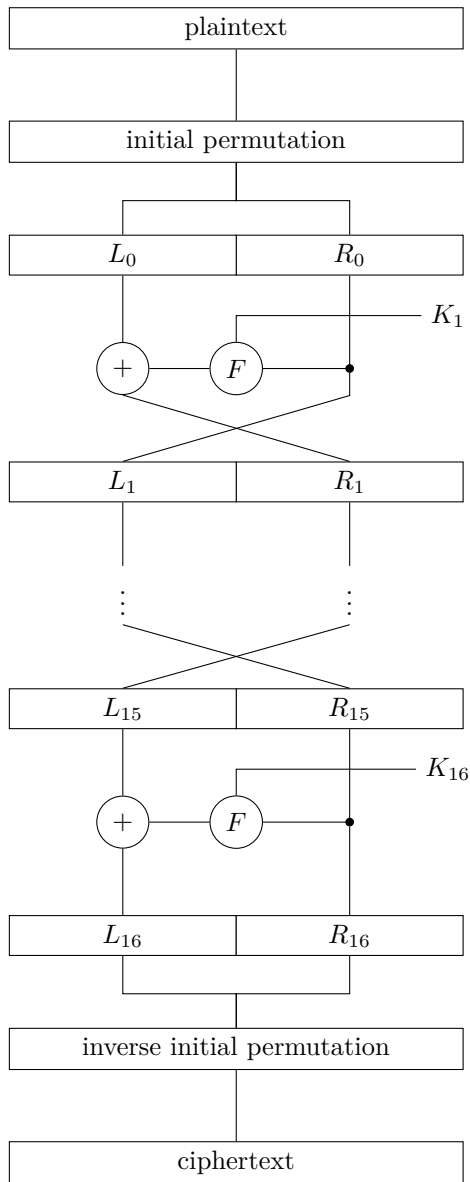
$$P = D_{K_1}[D_{K_2}(C)] \tag{B.2}$$

We have a key-space of  $2^{112}$  using two keys. The problem is that an attacker can reduce the key space quite drastically, provided that he knows a pair of ciphertext and plaintext. The rationale is to compute

$$x = E_{K_1}(P) \forall K_1 \in \{0, 1\}^{56} \tag{B.3}$$

$$y = D_{K_2}(C) \forall K_2 \in \{0, 1\}^{56} \tag{B.4}$$

and store one variable in a lookup table and compare against the other successively looking for matches. When a match is found you have two candidate keys for  $K_1$  and  $K_2$ . Computing the table require  $\mathcal{O}(2^{56})$  DES encryptions. This is done twice, so the overall complexity for the DES calculation is  $\mathcal{O}(2^{57}) = 2 \cdot 2^{56}$ . The lookup table will also require storage space  $\mathcal{O}(2^{56})$ .



**Figure B.2:** DES round structure

### B.1.2 3DES keying

The plaintext is encrypted using key  $K_3$ . The output from this round is decrypted using key  $K_2$ . The output from this round is encrypted again using key  $K_1$  to

produce the final ciphertext. This setup is the same for every keying option; the difference lies in how the  $K$ s are defined.

### Option 1, three independent keys

Using this keying scheme, all three keys are independent,  $K_1 \neq K_2 \neq K_3$ , giving us 168 bits of keying material.

$$C = E_{K_1}[D_{K_2}[E_{K_3}(P)]] \quad (\text{B.5})$$

$$P = D_{K_3}[E_{K_2}[D_{K_1}(C)]] \quad (\text{B.6})$$

### Option 2, two independent keys

Using this keying scheme we have  $K_1 = K_3 \neq K_2$  giving us 112 bits of keying material.

$$C = E_{K_1}[D_{K_2}[E_{K_1}(P)]] \quad (\text{B.7})$$

$$P = D_{K_1}[E_{K_2}[D_{K_1}(C)]] \quad (\text{B.8})$$

### Option 3, the same key

Using this keying scheme we have  $K_1 = K_2 = K_3$  giving us 56 bits of keying material. Using the given encryption function, this reduces to plain DES, as the decryption removes the first encryption.

$$C = E_{K_1}[D_{K_2}[E_{K_1}(P)]] = E_{K_1}(P) \quad (\text{B.9})$$

$$P = D_{K_1}[E_{K_2}[D_{K_1}(C)]] = D_{K_1}(C) \quad (\text{B.10})$$

## Discussion of keying options

Option 3 is provided to support legacy systems that only support one-key DES. Option 2 is an effort to increase the difficulty of performing a Meet in the Middle (MITM) attack over 2DES and option 3 gives even more key-space compared to option 2.

## B.2 Weak keys

*Weak keys* are cryptographic keys that make the cipher behave in a way that significantly reduce the strength of the cipher. As an example of such undesired behavior - DES has 4 keys where the encryption function is the same as the decryption function [26].

$$C = E_{K_1}[E_{K_1}(P)] = P \quad (\text{B.11})$$

The four keys that have this property are listed in listing B.1. The key is first shown in hexadecimal notation, followed by the binary representation. Notice that the key is 64 bits long and that the last bit in every byte is a parity bit.

```

010101010101010116
00000001000000010000000100000001000000010000000100000001000000012

FEFEFEFEFEFEFE16
1111111011111101111111011111101111110111111011111110111111011111102

1F1F1F1F1F1F1F16
00011111000111110001111100011111000111110001111100011111000111112

E0E0E0E0E0E0E016
11100000111000001110000011100000111000001110000011100000111000002

```

**Listing B.1:** DES weak keys. From [21]

Along with the four keys listed in listing B.1, DES has six key-pairs where encrypting with the first key and encrypting again with the second key will effectively decrypt the message. These are referred to as *semi-weak* keys. The keys are not listed here but can be found in [26].

When building applications that use DES one should be aware of this problem. Since 2DES and 3DES build on the same principles as ordinary DES, the problem of weak keys will still be present. If the key is generated at random, the probability of picking one of the ten keys mentioned above is not very big,  $\frac{10}{2^{64}} \approx 5.42 \cdot 10^{-19}$ . On the other hand, the list of weak keys is not that big and it is still good practice to verify that the generated key is not weak.







# Appendix **C**

## **AutoPASS example contract (Fjellinjen)**

Enclosed in figure C.1 is Fjellinjen's AutoPASS user contract.

 <b>AutoPASS-avtale</b> www.autopass.no		Besøksadresse: St. Olavsgate 28 Postadresse: Pb. 459 Sentrum 0105 Oslo Telefax: 22 11 68 55 Telefon: 815 00 101	 <b>FJELLINJEN AS</b> www.fjellinjen.no
<b>1. Generelt</b> SKRIV TYDELIG INNENFOR RAMMENE. BRUK BLOKKBOKSTAVER.			Kundenummer / Avtalenummer (7 siffer)
<input type="checkbox"/> Tegne avtale <input type="checkbox"/> Endre bilnummer <input type="checkbox"/> Endre adresse <input type="checkbox"/> Si opp avtalen <input type="checkbox"/> Bytte/Erstatte brikke <input type="checkbox"/> Meldte ut (av samleavtale)			<input type="text"/>
Etternavn (Firmanavn for firmakunde)			
<input type="text"/>			
Fornavn (Kontaktperson for firmakunde)			
<input type="text"/>			
Adresse (Fyll ut ny adresse her ved adresseendring)			
<input type="text"/>			
<input type="text"/>			
Postnr		Poststed	
<input type="text"/>		<input type="text"/>	
Land			
<input type="text"/>			
E-post			
<input type="text"/>			
Tlf. dagtid		Fødselsdato (6 siffer: DØMMÅÅ) (Org. nr. (9 siffer))	Bankkontonummer (for evt. refusjon ved avtaleendring og oppsigelse)
<input type="text"/>		<input type="text"/>	<input type="text"/>
<b>2. Gjelder for</b>			
Nytt bilnummer		Bilmerke	Startdato (Avtale / Endring skal gjelde fra dato)
<input type="text"/>		<input type="text"/>	<input type="text"/> Dag <input type="text"/> Mnd <input type="text"/> År <input type="text"/>
Klasse		Bilnr nasjonalitet	Annen nasjonalitet
<input type="checkbox"/> Lett motorvogn Maks tillatt totalvekt t.o.m 3500 kg <input type="checkbox"/> Tung motorvogn Maks tillatt totalvekt f.o.m 3501 kg Fritak (må dokumenteres) <input type="checkbox"/> El-bil / Hydrogenbil <input type="checkbox"/> Utrykningskjøretøy / Buss i konsesjonert rute / Forflytningshemmede		<input type="checkbox"/> Norsk <input type="checkbox"/> Dansk <input type="text"/>	<input type="checkbox"/> Svensk <input type="checkbox"/> Finsk <input type="text"/>
Eksisterende / gammelt bilnummer		Brikkenummer	Fest merkelappen fra brikken i dette feltet Kort brikkenummer (på formen L: xx xxxxxx x) L: <input type="text"/>
<input type="text"/>		<input type="text"/>	<input type="text"/>
<b>3. Gjelder for (bil nr 2)</b> Fyll ut ved nytegning av 2 biler på privatavtale.			
Nytt bilnummer		Bilmerke	Startdato (Avtale skal gjelde fra dato)
<input type="text"/>		<input type="text"/>	<input type="text"/> Dag <input type="text"/> Mnd <input type="text"/> År <input type="text"/>
Klasse		Bilnr nasjonalitet	Annen nasjonalitet
<input type="checkbox"/> Lett motorvogn Maks tillatt totalvekt t.o.m 3500 kg <input type="checkbox"/> Tung motorvogn Maks tillatt totalvekt f.o.m 3501 kg Fritak (må dokumenteres) <input type="checkbox"/> El-bil / Hydrogenbil <input type="checkbox"/> Utrykningskjøretøy / Buss i konsesjonert rute / Forflytningshemmede		<input type="checkbox"/> Norsk <input type="checkbox"/> Dansk <input type="text"/>	<input type="checkbox"/> Svensk <input type="checkbox"/> Finsk <input type="text"/>
Eksisterende / gammelt bilnummer		Brikkenummer	Fest merkelappen fra brikken i dette feltet Kort brikkenummer (på formen L: xx xxxxxx x) L: <input type="text"/>
<input type="text"/>		<input type="text"/>	<input type="text"/>
<b>4. Bruksområde / Reservasjon</b> AutoPASS i andre anlegg		<b>5. Avtaletype</b>	<b>7. Årsak til bytte / erstatning av brikke</b> Ved bytte av brikke hos forhandler skal det alltid betales nytt depositum for utlevert brikke. Depositum for eksisterende brikke vil bli refundert til oppgitt bankkontonummer.
<input type="checkbox"/> Jeg ønsker å reservere meg mot bruk i andre anlegg <small>Se veiledning</small> <input type="checkbox"/> Jeg ønsker at bruk i andre anlegg faktureres separat		<input type="checkbox"/> Privat-avtale <input type="checkbox"/> Firma-avtale	<input type="checkbox"/> Brikke stjålet / mistet / defekt ødelagt / dårlig batteri <input type="checkbox"/> Brikke innlevert
<b>Underskrifter</b> Jeg aksepterer herved Generelle og Spesielle avtalebetingelser samt Veiledningen vedlagt Avtaleskjema.		<b>6. Sletting av data</b> <input type="checkbox"/> Jeg ønsker at opplysningene om mine passeringer skal slettes når de er belastet avtalen.	SkjemalD: <b>25730</b>
Dato		Fyller ut av Bomselskap / forhandler	Forhandlerstempel
<input type="text"/>		Avtaledato	<input type="text"/>
Kundens signatur		<input type="text"/> Dag <input type="text"/> Mnd <input type="text"/> År <input type="text"/>	<input type="text"/>
<input type="text"/>		Forhandlernummer	Forhandlersignatur
<input type="text"/>		<input type="text"/>	<input type="text"/>

Avtalen leveres en av våre forhandlere

Versjonnr. 103 007

Figure C.1: Fjellinjen's AutoPASS user contract

# Appendix **D**

## RSA and blind signatures

*Blind signatures* are a scheme where one can obtain a signed digital message without revealing the contents of the message to the signing entity. An example of such a blind signature scheme is given for the RSA public-key algorithm. A description of the RSA scheme is given in section D.1 to together a blind signature scheme based on RSA in section D.2.

The original paper on RSA can be found here [33].

### D.1 RSA

Choose two random prime numbers  $p$  and  $q$  of similar length.  
Calculate

$$n = p \cdot q \tag{D.1}$$

$$\phi(n) = \phi(p) \cdot \phi(q) = (p - 1) \cdot (q - 1) \tag{D.2}$$

Choose  $e$  where

$$1 < e < \phi(n) \text{ and } \gcd(e, \phi(n)) = 1 \tag{D.3}$$

Calculate a multiplicative inverse  $d$  of  $e \bmod (\phi(n))$

$$d^{-1} \equiv e \bmod (\phi(n)). \text{ Equivalently } d \cdot e \equiv 1 \bmod (\phi(n)) \tag{D.4}$$

$e$  is known as the public key and is made public.  
 $d$  is known as the private key and is kept secret.

Encrypting a message to receiver A( $d, e, pq = n$ )

$$c \equiv M^e \pmod{n} \quad (\text{D.5})$$

where  $M$  is the plaintext message transformed into an integer and padded according to a padding scheme.  $e$  is A's public key.

Decrypting a message at receiver A( $d, e, pq = n$ )

$$M \equiv c^d \pmod{n} \quad (\text{D.6})$$

where  $d$  is A's private key.

## D.2 Blind signatures (With RSA)

Choose a random number  $r$  relatively prime to  $n$ . Calculate the blinded message

$$M_b = M \cdot r^e \pmod{n} \quad (\text{D.7})$$

Send  $M_b$  to signing authority. The message is signed with the signing authority's private key

$$S_b = M_b^d \pmod{n} \quad (\text{D.8})$$

$$= M^d \cdot (r^e)^d \pmod{n} \equiv M^d \cdot r \pmod{n} \quad (\text{D.9})$$

Note that  $r^{ed} \equiv r \pmod{n}$ .

The message is sent back to the user. With knowledge of  $r$  the user removes the blinding factor to obtain the signed message

$$S \equiv S_b \cdot r^{-1} \pmod{n} = M^d \cdot r \cdot r^{-1} \pmod{n} \rightarrow S \equiv M^d \pmod{n} \quad (\text{D.10})$$