1-1-2000

The potential use of smart cards in vehicle management with particular reference to the situation in Western Australia

Harry W. Jones

Edith Cowan University

USE OF THESIS

The Potential Use of Smart cards in Vehicle Management

with

Particular Reference to the Situation in Western Australia

By

Harry W. E. Jones BA., Grad Dip Cptr Sci

A thesis submitted in partial fulfillment of the requirements for the award of Master of Science

Faculty of Communications, Health & Science

20 November 2000

Abstract

Vehicle management may be considered to consist of traffic management, usage control, maintenance, and security. Various regulatory authorities undertake the first aspect, fleet managers will be concerned with all aspects, and owner-drivers will be interested mainly in maintenance and security. Car theft poses a universal security problem. Personalisation, including navigational assistance, might be achieved as a by-product of an improved management system. Authorities and fleet managers may find smartcards to be key components of an improved system, but owners may feel that the need for improved security does not justify its cost. This thesis seeks to determine whether smartcards may be used to personalise vehicles in order to improve vehicle management within a forseeable time and suggest when it might happen. In the process four broad questions are addressed.

- First, what improvements in technology are needed to make any improved scheme using smartcards practicable, and what can be expected in the near future?
- Second, what problems and difficulties may impede the development of improved management?
- Third, what non-vehicle applications might create an environment in which a viable scheme could emerge?
- Finally, is there a perceived need for improved vehicle management?

The method involved a literature search, the issue of questionnaires to owner-drivers and fleet managers, discussions with fleet managers, the preparation of data-flow and state diagrams, and the construction of a simulation of a possible security approach. The study concludes that although vehicle personalisation is possible and desirable it is unlikely to occur within the next decade because the environment needed to make it practicable will not emerge until a number of commercial and standardisation problems that obstruct all smartcard applications have been solved.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

9th April, 2001.

ACKNOWLEDGEMENTS

This thesis could not have been completed without assistance and contributions from many people, more numerous than can be explicitly mentioned.

However, my especial thanks go to Dr Thomas O'Neill, my principle supervisor, for patiently reading every word, guiding my ideas and research and correcting my convoluted phraseology.

Thanks also to Professor Anthony Watson, my co-supervisor, for suggestions, sources and authorisation of necessary materials acquisition.

Colleagues in academia and TAFE, officials in half a dozen Government departments and executives in as many industrial organisations assisted with information and advice.

I cannot forget the 85 drivers who, on Perth's hottest day of the year, took the time to answer my questionnaire before driving off.

Finally, thank you to Julie, my patient wife who has supported me throughout this effort and many others.

Table of Contents

Page

Copyright and access declaration ii
Abstract iii
Author's Declaration v
Acknowledgements vi

Chapter

1 INTRODUCTION 1

1.1 Inspiration for the topic - smartcards in cellular telephones 1
1.1.1 Personal communications and personal mobility 1
1.1.2 Electronic control and smart cards 2
1.1.3 Communications and mobility contrasted 2
1.1.4 Vehicle ownership in WA 3
1.2 Components of Vehicle Management 4
1.2.1 Traffic Management 4
1.2.2 Usage 7
1.2.3 Maintenance 9
1.2.4 Security 9
1.3 Perception of the need for better management 11
1.4 Thesis approach 12
1.4.1 Assumption. political will 12
1.4.2 Assumption. "killer application" 13
1.4.3 Assumption. multi-application smart cards 14
1.4.4 Factors impeding smart card research 14
1.5 Research questions 16
1.5.1 Necessary technological advances 16
1.5.2 Problems impeding development 18
1.5.3 Potential 18
1.5.4 Perceptions 19
1.6 Thesis structure 21

2 CURRENT RELEVANT TECHNOLOGIES 22

2.1 Introduction 22
2.2 Smart Card Capabilities 22
2.3 Present Smart Card Technology 24
2.3.1 Definition 24
2.3.2 Standards 25
2.3.3 Contact cards 26
2.3.4 Contactless cards 27
2.3.5 Card population 27
2.3.6 Card manufacture and system development 28

2.3.7 Manufacturing process 28
2.3.8 Cost and cost estimation 29
2.3.9 Present day cards 30
2.3.10 Conclusion 31
2.4 Biometric identification technology 31
2.4.1 Identification in general 31
2.4.2 Identification and verification 32
2.4.3 Smart card identification 34
2.4.4 Biometric performance 34
2.4.5 Comparison threshold 35
2.4.6 Template vulnerability 36
2.4.7 Biometric features 36
2.4.8 Fingerprint 36
2.4.9 Voiceprint 37
2.4.10 Eye retina 38
2.4.11 Back of hand 38
2.4.12 Comparison 38
2.4.13 Scanners 39
2.4.14 Pattern recognition 40
2.4.15 Conclusion 42
2.5 Transponders and access tokens 43
2.5.1 Description 43
2.5.2 Vehicle tracking application 44
2.5.3 Disadvantages 44
2.5.4 A different system 45
2.6 Passwords and PINs 45
2.7 Potential for Improved Smart Cards 46
2.7.1 Design constraints 46
2.7.2 Leading manufacturers and products 47
2.7.3 Basic or "no frills" designs 50
2.7.4 A de-luxe design 50
2.7.5 Contactless card potential 52
2.7.6 Memory size 52
2.7.7 Reading distance 53
2.7.8 Data transfer rates 53
2.7.9 Dual chip cards 54
2.7.10 Combi/Dual Interface cards 54
2.7.11 Other potential advances 55
2.7.12 More compact rewritable memory 56
2.8 Conclusions 56

3 SMARTCARDS & VEHICLE MANAGEMENT 58

3.1 Introduction 58
3.2 Traffic Management 59
3.2.1 General 59
3.2.2 Behaviour monitoring 59
3.2.3 Black box 61
3.2.4 Road fee collection 61

3.2.5 Parking fee collection 63
3.2.6 Pollution and congestion control 63
3.2.7 Vehicle related purchases 64
3.3 Usage control 65
3.3.1 Journey records and vehicle handling 65
3.4 Maintenance 66
3.5 Vehicle Security 66
3.5.1 General 66
3.5.2 Standards 67
3.5.3 Perimeter security 68
3.5.4 Alarms and immobilisers 68
3.5.5 Multi-point immobilisation 71
3.5.6 Aids to recovery 71
3.6 Improved convenience 72
3.7 Conclusions 73

4 PROBLEMS AND DIFFICULTIES 74

4.1 Introduction 74
4.2 Multiple application smart cards 74
4.3 Standardisation 76
4.3.1 Objectives and obstacles 76
4.3.2 ISO standards 77
4.3.4 Standard card operating system 78
4.3.5 MULTOS 79
4.3.6 Windows for smart cards 80
4.3.7 Java API 80
4.3.8 Backend software 82
4.3.9 Electronic payment standards 83
4.3.10 Common electronic purse specification 85
4.3.11 PC/SC specification 85
4.3.12 MIFARE 86
4.3.13 Other standards organizations 86
4.3.14 Certification authority model 87
4.4 Economic considerations 88
4.4.1 Cost estimation 88
4.4.2 Components of system costs 88
4.4.3 Card costs 89
4.4.4 Components of card costs 90
4.4.5 Other costs 91
4.4.6 Cost trend 91
4.5 Card capacity and performance 91
4.5.1 Required capacity 91
4.5.2 Extensibility and personalisation 92
4.6 Security 93
4.6.1 Aspects of security 93
4.6.2 Systemic 94
4.6.3 Chip level 95
4.6.4 Chip cracking 97

4.6.5 Counterfeiting 99
4.6.6 Card 100
4.6.7 Application 100
4.6.8 Security certification 101
4.7 Biometrics 101
4.7.1 Performance 101
4.7.2 Certainty of uniqueness 103
4.7.3 User acceptance 103
4.7.4 Testing 104
4.7.5 Industry testing and certification 105
4.8 Political and individual concerns 106
4.8.1 General 106
4.8.2 Tax avoidance 106
4.8.3 Hot money 106
4.8.4 Dirty money 107
4.8.5 Consumer choice 108
4.8.6 Consumer protection 108
4.9 Privacy and surveillance 109
4.9.1 Perception of privacy 109
4.9.2 Surveillance 110
4.9.3 Control of personal data 110
4.9.4 Unjustified identification 111
4.9.5 Vehicle identification 113
4.10 Resistance to change 114
4.11 Conclusions 114

5 COMMERCIAL ATTITUDES AND POTENTIAL APPLICATIONS 116

5.1 General 116
5.2 The smartcard industry "stakeholders" 116
5.3 Financial applications 119
5.3.1 Transactions generally 119
5.3.2 Bank attitude 120
5.3.3 Cash transactions 121
5.3.4 Electronic purse definition 122
5.3.5 Electronic purse contenders 122
5.3.6 Accrual transactions 124
5.3.7 Hot money 125
5.3.8 E-commerce 125
5.3.9 E-tailing 126
5.3.10 Security problems with e-shopping 128
5.3.11 Summary 129
5.4 Telecommunications 130
5.5 Oil companies 130
5.6 Major retailers 131
5.7 Entertainment 132
5.8 Local authorities 132
5.9 Federal and state governments 134
5.9.1 Road pricing 134

5.9.2 Public transport ticketing 135
5.9.3 Health 136
5.9.4 Welfare 137
5.10 Conclusions 137

6 SPECIFIC INVESTIGATIONS 139

6.1 General 139
6.2 Non-volatile, rewritable memory estimation 139
6.3 Vehicle fleet manager opinions 151
6.4 Security and a simulation 152
6.5 Security cost and perceived benefits 158
6.5.1 Perceived need for security 158
6.5.2 Cost of smart card facilitated vehicle security 159
6.6 Summary 160

7 RESULTS & PREDICTIONS 162

7.1 General 162
7.2 Required improvements. 163
7.2.1 Chip architecture 163
7.2.2 Chip improvements 164
7.2.3 Card manufacture and chip embedding 167
7.2.4 Biometric identification 168
7.2.5 Vehicle management 168
7.3 Technical expectations 169
7.3.1 General 169
7.3.2 Circuit density and size 170
7.3.3 Power supply 170
7.3.4 Memory 171
7.3.5 Contactless requirement 173
7.3.6 Biometric identification 174
7.3.7 Summary 175
7.4 Possible progress in overcoming non-technical difficulties 176
7.4.1 Standardisation 176
7.4.2 Cost reduction 176
7.4.3 Improved chip and transition to it 177
7.4.4 FRR reduction 178
7.4.5 Biometric ID method industry certification 179
7.4.6 Contactless card costs 180
7.4.7 Vehicle security and cost 180
7.4.8 Summary 181
7.5 Regulatory expectations 181
7.5.1 Traffic regulation enforcement 181
7.5.2 Road pricing and parking fees 182
7.5.3 Minor control improvements 184
7.5.4 Summary of traffic regulation prospects 185
7.5.5 General government applications 185
7.6 Commercial expectations - non-vehicle 186

7.6.1 Introduction 186
7.6.2 The purse and banks versus merchants 187
7.6.3 Payment standards 189
7.6.4 Purse battle 190
7.6.5 Internet payment protocols 190
7.6.6 Public transport ticketing 192
7.6.7 Telecommunication 193
7.6.8 Purely access applications 195
7.6.9 Welfare benefits 196
7.6.10 Health 196
7.6.11 Border control 197
7.6.12 Multiple applications 198
7.6.13 Holders versus issuers 199
7.6.14 Operating system compatibility 199
7.6.15 Public key certification 200
7.6.16 Holder certification 201
7.6.17 Summary 201
7.7 Industry forecasts 202
7.8 Perceived need for better vehicle management 210
7.9 Conclusion 212

REFERENCES 214
BIBLIOGRAPHY 227

Appendices

1 Determination of proportion of fleet vehicles 230
2 The crime environment 231
3 Vehicle and vehicle related theft 233
4 Estimating global monetary flows 237
5 System Repository 243
6 Questionnaire for fleet managers 249
7 Pascal code to manipulate smartcard reader 251
8 Microcontroller assembler code for HC11 254
9 Questionnaire for owner-drivers 258
10 Acronyms 259

Figures

1. Validation & verification 33
2. Receiver operating curves 35
3. Visual indication of biometric system merits 39
4. World finance & commerce in perspective 127
5. Data flow diagram – Context diagram 142
6. " - Level 0 diagram 143
7. " - Diagram 2 Enroll owner drivers 144
8. " - Diagram 3 Transmit data 145
9 " - Diagram 4 Poll vehicle sensors 146
10. " - Diagram 5 Identify driver 147
11. " - Diagram 6 Extract logged data 148
12. " - Diagram 7 Manage engine & personalise data 149

13. Security State Diagram 153
14. The Simulation block diagram 154
15. The Simulation as built 156
16 An idealised smart card architecture 164
17. Required chip features 166
18. Graphical portrayal of smart card estimates and forecasts 209

Tables

1. Prominent smart card chips 49
2. Magstripe and smart cards compared 89
3. Magstripe smart cards and optical cards compared 90
4. Smart card costs 90
5. Card memory requirement 151
6. What motorists might pay for security 160
7. Required and available chip features 166
8. Telecommunication industry smart cards 193
9. Schedule of estimate and forecast references 205

1 INTRODUCTION

1.1 Inspiration for the topic - smart cards in cellular telephones

1.1.1 Personal communications and personal mobility.

Within the last century there have been dramatic improvements in personal communications. One hundred years ago only the rich had telephones and usage was limited to local calls: long distance messages were sent by telegraph. Today, with a cellular telephone, it is possible to communicate with another person almost anywhere in the world; however, minor nuisances such as unwanted interruption and disturbance for others nearby have accompanied this improved convenience. In contrast, there have been lesser improvements in personal mobility. The vehicle, the principal personal mobility device, is less convenient and has become more of a nuisance. Can we enhance its convenience and overcome the nuisance factors of security risk, wasteful usage, pollution and crowding? Perhaps, in the distant future, in potentially hazardous traffic situations such as major intersections, an automatic system might assume control of all vehicles within a specified zone and regulate their speeds and distances to improve efficiency and safety by the temporary suspension of the human factor. As an ultimate example, might we, one day, match the convenience of the cellular telephone and have our car at our fingertips, summoning it like a magic carpet from elsewhere, by pressing buttons, and dismissing it in the same way?

1.1.2 Electronic control and smart cards

The magic carpet concept is lent a tinge of credibility by the worldwide trend towards electronic control and delivery in commerce. This trend is apparent in financial, telephone, transportation, utility, entertainment, health, and welfare, systems. An example is the application of Subscriber Identity Module (SIM) cards in Global System for Mobile communication (GSM) cellular telephones that has shown how useful a smart card may be in personalising a device for the individual. It is possible that, just as a person inserting his/her SIM card into any compatible cell phone makes that phone his/her own, a smart card might contribute to personalising a motor vehicle for its owners or drivers. In this thesis the term "smart card" is reserved for cards that conform to Parts 1 to 6 of the International Standards Organisation (ISO) standard 7816 and may serve as both a source and a repository of data, and/or as a highly portable processor. Standard ISO 7816 is discussed in more detail in section 4.3.2. The smart memory card, whose processor merely controls its memory with "hard wired" logic, is excluded.

1.1.3 Communications and mobility contrasted

Although the need for vehicle personalisation may be similar to that accepted at present for cellular telephones, there are differences between personal communication systems and personal mobility ones. Telephone channels are owned privately, or by a government agency, and the owner has almost absolute control over them, but Australian roads are generally publicly owned and control is mostly a matter of prohibitions. The reasons for the differences are practical, rather than logical, and it is possible that one day a national government might privatise more roads, and the new owners impose a toll or traversal fee, as is the practice in Singapore and in some places in the US and France today. Another possibility might be that the Internet absorbs the global telecommunication network, with most intelligence and control becoming resident in the terminals rather than the network nodes. So, we may see a convergence between the communication and mobility systems. In the author's opinion, personalisation will probably remain as a major attraction for users, and smart cards appear to be the best tool for its implementation. Whatever happens, smart cards might play an increasing role and the following discussion examines this possibility.

1.1.4 Vehicle ownership in WA

Before defining vehicle management, its scope should be estimated. At the 1998 census, Western Australia (WA) had about half a million cellular telephones and about 1.1 million passenger and light commercial vehicles, of which the vehicles constituted a vastly greater asset (Yearbook Australia, 2000, p. 602). Included in the 1.1 million are both fleet and owner-driven vehicles. For fleet vehicles, accountability for their efficient employment usually rests with someone other than the driver. Of cars and light commercial vehicles, a majority are personal transport and owned by the driver or driver's family; whereas, the remainder, about ten percent (see Appendix1), might be regarded as fleet vehicles, where the driver(s) are not necessarily the owner(s). This fleet versus private distinction is not clear-cut, as many cars are family transport and driven by more than one member of the family. Since the drivers of fleet vehicles may have no direct stake in efficiency, a more formal and controlled management style is required for such vehicles than for those driven by their owners. However, it seems likely that any management system that gains widespread acceptance will have appeal to the private, as well as the fleet, owner.

1.2 Components of Vehicle Management

Vehicle management may be considered to consist of traffic management, usage control, maintenance, convenience and security. These components have associated problems that are described next, and that might be ameliorated by a smart card supported system.

1.2.1 Traffic Management

Traffic management presents problems in behaviour, congestion and pollution, and in the provision of parking spaces. These problems are now examined in the light of trends in vehicle management and usage: furthermore, potential business opportunities are highlighted.

Behaviour control includes determination of regulations, registration of vehicles, licensing of drivers, monitoring and enforcement. Even with the increasing employment of multi-novas (speed cameras that are operated by police auxiliaries) for speed control, the surveillance that results is intermittent and currently, in Australia, monitoring of roadworthiness is not comprehensive. Recently, a subsidiary problem, the identification of those who exceed speed limits, has captured media attention ("Privacy fear", 1999). A system that automated monitoring and ensured identification might improve behaviour.

Some congestion, with accompanying pollution, is inevitable, as the utilisation of cars in WA is neither static nor declining: for example, there was a steady rise in the number of registere.l vehicles throughout 1995-1997 (Yearbook Australia, 1998, p. 600). Naturally, this rise adds to the congestion and pollution problems, as the Australian Federal and State Governments cannot provide, in the short term, for the increasing number of vehicles by constructing extra roads due to private land ownership limiting the availability of appropriate space. The Federal and/or WA State Government response may exploit the general trend in fiscal policy to make the user (especially, the motorist) pay. The trend has been given prominence with the High Court ruling concerning 'he right of Australian States to impose a tax on petrol (Sources of State Revenue, 1999). The issue of road pricing, as an effective means of both managing road traffic demand and raising additional revenue for road construction, is on the political agenda of many European governments (Blythe, Burdon, Clark, Givens & Rourke, 1994, p. 42). For example, in some cities, such as Singapore, a charge is made on every motorist who enters the central business district. Australian governments have not ignored the trend. National and State projects are described in section 7.5.2. Congestion might also be reduced if smart cards were used to encourage car-pooling and facilitate cost sharing between vehicle occupants.

Motorists expect to pay for parking in congested areas, and there is a perception that user payment is the fairest way to allocate a scarce resource: this perception is reinforced by the needs of local bodies. Parking fees and fines resulting from parking offences are an important source of revenue for civic authorities, particularly as their imposition may also advance the socially desirable objectives of reducing pollution and congestion. Australia wide, in 1995, parking was an 80 million-dollar industry (Guimmarra, G. & Luk, J, 1995). Currently, coin-operated kerb-side devices or ticket dispensing machines collect the fees and, in either case, wardens must monitor the system. Mechanical meters are vulnerable to vandalism and theft, have unreliable moving parts, and provide no information about the cash collected (Luk, J.Y.K., 1995, p. 1).

For both behaviour control and parking, the present method of collecting traffic management charges is labour intensive, expensive and, therefore, wasteful: hence, a system that could collect the charges automatically and accurately would be desirable. The introduction of any automatic system would depend on the existence of a "critical mass" of motorists prepared to pay for the necessary roadway and "in-vehicle" devices; however, until there is a mass market for the devices, their prices would continue to remain high and the "critical mass" might not eventuate. An example of this possibility is the "City Link" project in Melbourne which is reported to be functioning satisfactorily (City Link Project, 1999). Prices might fall and the transition to widespread automatic collection systems be facilitated if fuel companies, road authorities, and financial institutions, cooperated to standardise the collection method. In this regard, smart cards might provide the facilitating mechanism for such a standard automated "user pays" system. Standardisation is considered in more detail in chapter four.

There may be problems in developing an automatic system, but there are also business opportunities. The number of fuelling and other transactions in vehicle usage is second only to point-of-sale transactions in the food industry (Arazi, 1991, p. 646). Arazi is probably referring to the US, and Australia does not collect a comparable statistic, but this admittedly dated reference is not inconsistent with statistics from the Household Expenditure Survey, Australia, Catalog No 6535.0. Since vehicles operate day and night, the gradual adoption of automatic vending would seem to be inevitable. Other opportunities include insurance sales and support, navigational information and, on a futuristic scale, a city hire car system along the lines of the Praxitele pilot scheme now under trial in Saint-Quentin en Yvelines, France (Arensonas, 1996).

1.2.2 Usage

In contrast to traffic management, usage is of more concern to owners, especially fleet owners, than to authorities. Owners are concerned about cost, and the operation of 1.1 million registered light vehicles is a significant cost. The Royal Automobile Club of WA (RAC) web site gives estimates of the cost per kilometre to run a vehicle as varying from about 80 cents for a Long Wheel Base (LWB) off-roader to 38 cents for a small city runabout ("Car running costs", 2001). An average figure might be about 50 cents and an average annual kilometres per vehicle might be about 15,200 (Yearbook Australia, 1998, p. 602). Therefore, the estimated cost of vehicle usage in WA might be about A$8.4 billion. The ten percent of vehicles that are in fleets, in practice are newer than those owned by individuals and are more heavily used; consequently, the cost of their operation is likely to be more than ten percent of the total.

Although owner-drivers might welcome some assistance in controlling use of their vehicles, the desire for assistance is unlikely to amount to a compelling motivation to purchase even a cheap device because the owner is entitled to "waste" resources in his/her vehicle if convenience so dictates.

For fleet owners the situation is different, since profit considerations require that the fleet provide the maximum benefit for the minimum cost. A one percent improvement in the management of a "A$1bn plus" annual expenditure of resources is a substantial sum that, although insignificant when compared to WA's Gross Domestic Product (GDP) of A$50b, might justify pressure to improve control (Australian Economic Indicators. p. 92). Control requires accurate records of what journeys a vehicle has made and why. Without some form of automation this is a tedious chore and the results are often not accurate, but automatic onboard loggers, whilst available, are expensive. At present fleet managers usually issue fuel cards to drivers knowing that the chosen fuel company records the details of cards that are tendered and, from a central database controlled by that company, will provide reports to the managers. Drivers may be required to keep additional details, such as the reason for the journey, in logbooks. The potential for automatic recording of these additional details in the convenient portable data stores provided by smart cards is obvious, and is considered in chapter three.

1.2.3 Maintenance

Control of maintenance, unlike traffic management and usage, offers little scope for exploiting personalising smart cards because maintenance relates to the vehicle rather than the user. The maker predetermines most of the maintenance activities. Nevertheless, a smart card system could provide reminders about periodic checks, or reports of incipient failure. Moreover, repairs under warranty and (to a lesser extent) maintenance depend on accurate recording of previously performed work and the reporting of defects. When vehicles are moved from one location to another a smart card system might help to ensure that records are available in the new locations. In the USA, the Environmental Protection Agency has regulations establishing requirements for on-board diagnostic (OBD) systems on light vehicles manufactured after 1993 ("Frequently asked questions", May 1997). These systems notify the driver of faults by means of a dashboard light. A non-owner driver might be tempted to ignore the light, but if the diagnoses were recorded on smart cards that were returned to the owner's office at prescribed intervals, it would be possible for the owner to arrange remedial action.

1.2.4 Security

Vehicle security, the final component of vehicle management, must be examined in the context of the crime environment as a whole. Crime statistics may be interpreted in different ways so the environment has been discussed in more detail in Appendix 2. Suffice to say here, that motorists should not be tolerant of vehicle-related theft merely because their insurance covers them against loss.

Before considering possible security measures it is sensible to examine the nature of the crime and seek answers to the following questions.

- Who steals cars and why?

  As a generalisation, car thieves probably fall into two fairly equal categories: young impulsive thieves and older cunning professional thieves (Biles & Willing, 1987, p. 42).

- What kind of car is most frequently targeted?

  The only clear trend is that older cars appear to be more frequently targeted (Devery, 1993; Motor vehicle theft in SA, 1995).

- How many are taken and where from?

  In WA, about 19,000 vehicles at a cost of A$80m to A$100m are stolen each year; therefore, the security aspect alone is worth study. Cars seem to be stolen impartially from all places to which the public has access (WA Police Annual Crime Statistics Report, 1995/96).

- How are they taken?

  Methods vary but human carelessness is a frequent contributory factor (Geason & Wilson, 1990; Devery, 1993).

More detailed responses to the above questions have been provided in Appendix 3.

A fairly simple and cheap method of security would probably foil impulsive thieves, but a more sophisticated defence would be needed to prevent a professional theft. Therefore, a basic system should be modular and extendible so that owners can get the level of security which they require. Ideally, retrofitting a system to older vehicles should be possible and the chosen system should compensate, as far as possible, for human carelessness. How smart cards might be part of such a system and also facilitate the tracking of stolen vehicles, is discussed in chapter three.

1.3 Perception of the need for better management

Whether a better system of vehicle management emerges may depend upon the public's perception of the need for improvement: but perceptions depend upon viewpoints. Although there may be a need for better management to promote individual control of mobility and remove, or at least reduce, currently experienced nuisance factors, the recognition of that need is not universal. For example, many people advocate a greater use of public transport; arguably the equivalent of a return from the telephone to the telegraph office. It will be argued that this lack of recognition is the major reason for the lethargic manner in which the problems obstructing progress, including problems of standardisation, have been addressed.

Generally, if vehicle ownership and usage continues to increase at the present rate, management will become both more difficult and more important whatever the awareness of the need. The management of traffic is fragmented amongst various authorities; usage control and maintenance seems to be an important issue only for fleet owners; and, security is probably the main concern of owner-drivers. Moreover, employed drivers are likely to be unenthusiastic about any proposal that adds to either their chores or their responsibilities. This fragmentation of viewpoints, contributing to the lack of any perceived need for improvement, is possibly the greatest obstacle to the development of a better system. Inharmonious motivations merely exacerbate the difficulties. Adopting a positive perspective, this thesis argues that intelligent people should overcome obstacles rather than surrender to them; but, it accepts the reality that, whilst any technology that promises improved efficiency will probably be investigated, identified technical enhancements may not be implemented. It would help if "in-vehicle" devices were modular in design so that motorists could get just those aspects for which they felt the greatest need. Another positive factor might be that, as a by-product of automatic systems, more information might become available to authorities, vendors and owners (e.g., times and places of payment). The recipients might welcome feedback, but drivers might regard it as an invasion of privacy. Since it is argued that perceptions are crucial in assessing the likelihood of developing a more personal mobility system, their assessment will be left to chapter seven.

1.4 Thesis approach

This thesis seeks to determine whether smart cards will be used to personalise vehicles, thus improving vehicle management within a foreseeable time frame. To improve the focus of the study, and explain what at first may appear to be omissions in the investigation, a number of assumptions are made and factors that impede smart card research generally are mentioned briefly.

1.4.1 Assumption - political will

A political will to attack road and traffic management more vigorously will be needed, but it is emerging only slowly. Attention has already been drawn to the fact that the highway used by a vehicle differs from the "highway" used by a cell phone in that:

- a non-commercial organisation usually owns a road,
- users do not usually need the approval of the road owner,
- vehicles are approved for road use by an organisation other than the road owner, and
- road management is less thoroughly covered by international agreement.

Amongst the consequences of these differences is that, unlike a cell phone SIM card system, a personal mobility system using smart cards probably cannot stand alone. First, Federal, State and local body road owners and regulatory authorities must cooperate to create a suitable road network. Second, the mobility system needs more technical support than a communication system, it would cost more, and individual motorists might not be prepared to meet this cost. Third, to provide more value to justify the cost, smart cards used in vehicles would need to be useable in card readers other than those in the vehicles. After considering these consequences the assumption has been made that, despite the technical possibility of managing roads in a manner similar to the management of telecommunication links, the environment to facilitate such management is developing only slowly. Progress may depend, in part, upon political decisions, but politicians are wary and wait for pressure from the electorate.

1.4.2 Assumption - "killer application"

The nature of the environment, within which a smart card supported vehicle management system might emerge, depends on commercial factors as well as the political ones already mentioned. With this dependence in mind, a second assumption has been made: namely, that the use of smart cards might explode if a "killer application" emerged to form the core of a multi-application card, whose acceptance might then achieve critical mass. Just as the word-processor and the spreadsheet were the commercial applications that brought the personal computer (PC) onto many desks, so some equivalent application may be needed to put a smart card in every wallet.

1.4.3 Assumption - multi-application smart cards

A smart card system would be unlikely to be used solely for vehicle management, therefore there would need to be space on the card for other applications and any associated problems in creating a multi-application smart card would have to be solved. Continuing the analogy with the PC, people may have bought a PC primarily for use as a word-processor but they became aware of its other uses, which they quickly began to exploit. For general acceptance a smart card, likewise, is assumed to need an extension potential.

1.4.4 Factors impeding smart card research

When experiment or direct observation cannot obtain answers to questions posed, for example queries involving the future behaviour of people, a review of literature is often the only possibility of enlightenment. When dealing with smart card research, even with this method there are difficulties due to commercial confidentiality. Two examples follow.

- Information obtained from the records of commercial organisations, or by market surveys, is valuable but costly and is seldom is released universally until it is severely dated.
- Technically comprehensive reports, based upon market research using commercially collected statistics, are expensive. Examples are "Smartcard Technology" by SJB Services and "Smart Cards in Transport" by Dean, Arnold & Harrop. In 1997 these texts each cost over A$1000 and still cannot be obtained from booksellers or borrowed from libraries. However, CardTechnology, an online magazine published by FaulknerGray, now releases some figures when they are no longer commercially valuable.

The World Wide Web has proved to be the most useful source of up-to-date information. Unfortunately, much of the information on the Web is anonymous and, as a source, is contaminated by hype and inaccuracies. Moreover, when informative and apparently authoritative Web pages are found, frequently they are posted only temporarily.

Journal articles, both those published on the Web and those located by Internet searches, tend to be either non-technical or non-specific in their treatment of commercial possibilities.

In addition to the literature sources described above, inquiries were made of the Police Department, the Crime Research Bureau of UWA, Westrail, the Insurance Council, the RAC, Main Roads WA, the Perth City Council, five major fleet owners and a number of vehicle immobiliser vending merchants. These organisations formally responded with caution to unwarranted requests for specific information.

1.5 Research questions

Four broad questions are addressed and, in the following subsections, these are each stated briefly and elaborated.

1.5.1 Necessary technological advances

What advances in technology are needed to make any improved scheme using smart cards practicable, and which of them may be expected within the time frame?

This main question can be divided into the following four subordinate questions.

- What general improvements might be needed in smart card chips to make them practicable and acceptable for a wide range of applications?

  Potentially improvable features are memory (especially RAM, EEPROM or other rewritable, non-volatile memory) power consumption and processing power.

- What do different levels of vehicle management (authorities, fleet operators, owner-drivers and users) demand in increased card memory capacity?
- What improvements might be needed in biometrics identification systems?

  Four potentially improvable aspects might be:

  - reductions in False Acceptance Rate (FAR), in False Rejection Rate (FRR), in invasiveness, in scanner size and in cost,

  - increases in reliability and flexibility (ranging from high security through to adequate deterrent),
  - easier enrolment of persons to be identified, and
  - improved and standardised testing.
- What vehicle modifications might be needed?
- What infrastructure (external to both card and vehicle) developments might be required?

In this thesis, in chapter 6, in pursuit of answers, a possible vehicle management system is modelled and data flow diagrams with supporting repository are prepared to enable an assessment of both the on-chip data storage required and, specifically for vehicle applications, the necessary rewritable non-volatile memory. In addition to these assessments, in section 6.2, a further estimate is made of the extra memory needed for other associated applications. To clarify the vehicle security requirement a state diagram is prepared identifying the different security states (locked and immobilised, unlocked but immobilised, ready and valet mode) and the transitions between them. A simulation of partial security aspects of a vehicle smart card system seeks to demonstrate the technical feasibility of such a system and the enhanced security it might provide, and hints at the prerequisite modifications and possibilities for smart card vehicle management. A search of the Internet and journals is carried out to assess the commercial and public expectations of biometric identification methods.

An attempt is also made to estimate within what time frame these technical advances (changes or improvements) might be expected.

1.5.2 Problems impeding development

What problems and difficulties might impede the development of personal mobility comparable to existing personal communications?

The envisaged problems and difficulties seem to be mainly non-technical and include excessive costs, inadequate card performance, flawed system security, unacceptable biometric rejection rates, failure to achieve standardisation, and political attitudes and fears. The political factors have almost total influence upon regulatory changes that might affect the environmental options, such as whether road pricing might conceivably be introduced and whether surveillance of motorists and enforcement of regulations should be intensified (possibly, to the extent currently the case with aircraft pilots). Inevitably, therefore, uncertainty exists as to what measures, if any, are likely to be taken to improve driving behaviour, to reduce traffic congestion, and to minimise pollution.

The problems of vehicle management are described in more detail in chapter 3. The general thrust of several discussion papers issued by the WA Department of Transport and a Web page issued by the NZ Government are outlined in section 3.2.

1.5.3 Potential

What potentially changing public attitudes and commercial developments might create an environment in which a viable scheme could emerge?

The thesis argues that changes, not directly related to vehicle management, might impact on the environment. Candidate developments include innovations in:

- finance (e.g., the electronic purse),
- transportation (e.g., public transport ticketing),
- telecommunication(e.g., for pay phones and e-commerce),
- authentication (e.g., for welfare benefits),
- storage of information (e.g., for health records), and
- other minor areas.

The possibility that any of these developments, or a combination of them, might result in smart cards becoming ubiquitous is evaluated and an opinion is formulated.

1.5.4 Perceptions

What is the public (political, commercial and individual) perception of the need for an improved personal mobility, including better vehicle management?

The investigation seeks to determine if there is a perceived need for improvement in vehicle management by regulatory authorities, fleet owners, individual vehicle owners, and/or drivers; and, if so, whether the perception in any way contemplates a system using smart cards. What owners (fleet or individual) might be prepared to pay for better vehicle management is accepted as an indication of perception. The extent that authorities might be prepared to impose a higher standard of behaviour on owners and drivers, and (in their turn) fleet owners upon drivers, is assessed, as also are vehicle owner perceptions of what is a cost-effective level of vehicle security.

It was decided that the best method for obtaining an indication of perceptions would be by questionnaires reinforced by direct interviews where possible, with opinions being sought from regulatory authorities, vehicle fleet owners, and owner-drivers. However, public officials cannot be expected to complete questionnaires which have not been approved by their superiors; so, necessarily, the determination of the views of regulatory authorities was confined to the informal discussions that were held with officials in the WA Department of Transport, Main Roads WA, and Perth City Council. The position of commercial managers is different and five Perth major fleet owners were contacted by telephone, sent a questionnaire, and asked for their opinions. All responded to the questions, but only verbally. For owner-drivers the situation is different again. To survey the opinions of visitors using the student car park at Edith Cowan University (ECU), Mount Lawley (MTL) campus, a questionnaire was distributed to almost 300 vehicle drivers. The form was placed under windscreen wiper blades and returned anonymously by various means. The questions specifically ask about desirable levels of security, and endeavour to obtain the views of individuals as to the cost-effectiveness of different levels, but a subsequent reinforcing interview would not have been feasible. What is known, is that ECU students include more part-time and mature students than other Perth Universities (Student's (Preliminary) Selected Higher Education Statistics, 2000, p. 27); therefore, the responses are likely to be fairly representative of the opinions of citizens in general. A search of trade magazines seeks to reinforce the views obtained by the questionnaires.

1.6 Thesis structure

It is now possible to describe the structure of the thesis. Chapter two examines the current state of the technologies that might promote better vehicle management and chapter three considers how these technologies might be applied. Chapter four examines problems and difficulties of a general nature, such as the obstacles to standardisation, costs, security and political and individual concerns; and, chapter five analyses commercial factors that might influence the adoption of any system. Chapter six describes investigations undertaken to answer questions that are not addressed in the literature: including an analysis of a possible system to estimate the card memory needed, a study of the opinions of fleet managers and owner-drivers and a simulation to demonstrate an approach to enhancing security. In chapter seven, conclusions are drawn, not only from the preceding discussion of positive and negative influences, but also from the opinions of authorities who are also trying to predict the future of smart cards. Finally, the seven chapters are supported by a number of appendices incorporating relevant technical and statistical detail.

2 CURRENT RELEVANT TECHNOLOGIES

2.1 Introduction

This chapter examines the current situation in smart card technology and the associated area of biometric identification; it briefly considers the alternatives for access control, such as transponders and passwords or PINs; and, it explores the possibility of developments that might lead to more widespread, perhaps even ubiquitous, use of the cards.

2.2 Smart Card Capabilities

A discussion of smart card technology should begin with a consideration of what the devices do, therefore potential general application categories are summarised before describing smart card, associated, and alternative, technologies. A report (Butler, 1996, p. 2) prepared by the New Zealand Futures Trust states:

> "There are three kinds of applications of smart cards:
>
> **Authentication.**
>
> This allows cardholders to gain access to buildings, facilities, databases etc. In general, these applications are convenient, secure and efficient and pose few problems for either users or providers. A number of such applications are already operating...

> **Stored-value transactions.**
>
> Here a smart card can be used as an electronic purse, which may also be reloadable. Before there is wide acceptance and use of stored-value cards for financial transactions, ... the public... will need to be convinced of: ...(a number of features)...
>
> **Store of information.**
>
> The third main use of smart cards is as portable records, to store information which needs to be independent of fixed locations, e.g. as a patient's health card, or for vehicle or equipment maintenance. As with stored-value transactions, questions of standardisation, privacy and security must be resolved before there is general acceptance".

Other authors, for example, Myers and Baker, broadly confirm this statement and although, seven years ago, Baker gave greater emphasis to security as the most important characteristic of smart cards, Baker's attitude is probably not inconsistent with the general application categories described above (Myers, 1996; Baker, T., 1992). Amongst electronic payment systems supported by smart cards, distinctions should be drawn between open and closed systems, and between electronic purses and stored-value cards (SVCs). A closed payment system is one in which the issuer of value in digital form is also the sole redeemer of that value: for example, a prepaid telephone card system. By contrast, in an open system a range of organisations and individuals may accept the digital value and provide goods or services in return without the prior knowledge of the issuer. At one time the terms SVC and electronic purse were regarded as synonymous, but, increasingly, a distinction is being made between SVCs that cannot be reloaded, and are commonly used in closed systems, and reloadable purses that are more suitable for use in open systems. This distinction makes sense, because, in ordinary parlance, a purse is a device into which we can put money for subsequent spending where we choose. Vehicle management, as described in the introductory chapter, has candidate applications in:

- authentication (e.g., security),
- stored-value transactions (e.g., vehicle related payments), and
- stores of information (e.g., record keeping).

The possible applications are explored in more detail in chapter three, whilst this chapter considers present day technology, both supportive and alternative, and the potential for improvements and refinements.

2.3 Present Smart Card Technology

2.3.1 Definition

There is some confusion about the definition of a smart card, but any card that incorporates a microcontroller is clearly a chip card. Chip cards can be divided into memory cards and smart cards.

- Memory cards have more memory than magnetic-stripe cards, and "hard-wired" programs to control that memory, but no processing capability.
- True smart cards have a facility that enables the chip to be partially reprogrammed after manufacture, and they have both read only memory (ROM) and other non-volatile memory; the latter usually stores the "smartness" of the

card in programs to calculate, encrypt, manipulate, and record, data. Also, the programs and data are stored in a type of non-volatile memory that can be read years later, and can be over-written many thousands of times. In turn, true smart cards can be divided into contact and contactless types: both are defined, in some aspects a little laxly, by international standards which are introduced in the next section. Contactless cards can be "close-coupled"/proximity/vicinity type which are readable at 1mm/10cm/1metre, respectively.

The terms hybrid, dual-chip and combi/dual interface are now used by authors, but not always consistently. A hybrid card has a magnetic stripe as well as smart card features; a dual-chip card, obviously, has two chips, one of which is accessed through a contact plate and the other using remote communication features; and, the combi/dual interface card has a single chip that can be accessed by contact or remotely.

2.3.2 Standards

Standard ISO 7810 prescribes the size of smart cards, and standards ISO 7816/10536 the nature of communications with contact/"close-coupled" contactless cards. A draft standard ISO 14443 for "remote-coupled" contactless cards has yet to be finalised and there is a proposal for standard ISO 15693 for vicinity cards. Initially, smart cards were designed for closed systems, such as prepaid telephone card systems, and their electrical properties were relevant only in so far as cards had to be compatible with their associated readers. Today, multi-application cards are considered to be desirable, and these types of card, eventually, will have to be capable of forming a matching pair (on a "one to one" basis) with many different terminals and readers. The need for wide compatibility became apparent with the growth of the GSM mobile telephone network. The electrical properties defined in the European Telecommunication standardisation Institute (ETSI) GSM 11.11 standard for the SIM card have become a model for semiconductor manufacturers and, in effect, have extended the conditions defined in standard ISO 7816-3 (Rankl & Effing, 1997). A list of ISO and other standards and specifications relevant to smart cards has been prepared by the Smart Card Forum and can be found at http://www.edtn.com/embapps/fancher-97-t1.htm. These and other standards are discussed in the chapter dealing with problems and difficulties (see chapter 4 section 3).

2.3.3 Contact cards

The integrated circuit chip on a contact smart card requires some input from the outside world and, generally, this input is an electrical voltage to power the chip and a clock frequency to synchronise chip activities. Another requirement is an input/output path for the transmission of data which, for the contact card, is created by direct connections established between card and reader. The integrated circuit on the chip is connected to a contact plate on the surface of the card and when the smart card is placed into a reader device, the card's contact plate is mated with connections in the reader to complete an electrical circuit. Clearly the contact plate must be in position as defined by standard ISO 7816-2.

2.3.4 Contactless cards

The contactless smart card dispenses with the contact plate on the surface of a smart card and instead uses some form of electronic coupling. Generally, contactless smart cards will be placed in close proximity to a reader and an inductive (transformer) or capacitive coupling is used to transfer energy and power the card. The clock may be internally derived and data transferred by modulating the power supply. Standard ISO 10536, mentioned earlier, is a fairly loose standard since different manufacturers use different methods, including either capacitive or inductive coupling, that are incompatible with one another ("Smartcard technology", 1994). It is still too early to assess the effect of standard ISO 14443, the planned standard for "remote-coupled" contactless cards.

2.3.5 Card population

In 1996, about 100 million smart cards were estimated to be in use. (Note: The comparable figure for chip cards was well over 500 million, but most, for example phone cards, were merely memory cards and did not meet the definition of true smart cards given above). By 1998, the number issued could have been over a billion. Bauer of Siemens claims that Europe currently holds the lion's share of the world smart card market (50%); but, according to estimates by its Semiconductor Group, the US may account for 25 % of the market by 1999. By the year 2000 Southeast Asia and Japan are expected to reach a 25 % market share (Bauer & Hamman, 1996). A table of forecasts is presented later, as Table 9, in chapter seven.

2.3.6 Card manufacture and system development

Several manufacturing industries have an interest in the smart card market. Firstly, chipmakers face challenges in making suitable chips; secondly, cardmakers have problems in integrating the chip and the card into a marketable product; and thirdly, a number of minor players are working to develop supporting devices, such as readers. However, card issuers are probably the stakeholders that are most important in determining the general acceptance of smart cards. Banks and other financial institutions must decide whether or not to exploit smart card technology; but, even as active participants, they may have difficulty in persuading users to accept their preferred products. Finance is a likely, but not the only possible, application field. For example, some authorities claim that by the end of the decade, about 50% of all smart cards will probably be used for transportation, either in contactless toll collection systems for expressways, or as combined entry and billing systems for public transit users, or as automobile entry systems, (Bauer & Hamman, 1996; Higgs, 1996). Discussion of the attitude of financial institutions and other potential issuers is deferred to the section dealing with commercial factors.

2.3.7 Manufacturing process

The process of manufacturing chips for smart cards is not greatly different from that used in manufacturing any other chip, except that special security precautions must be observed. More specifically, the design of the chip usually includes features to frustrate reverse engineering; all chips, both functional and faulty, must be accounted for; and, the delivery process is similar to that used for bullion (Paterson, 1991, p. 36). Manufacture involves using a series of masks to etch circuitry onto silicon wafers and, usually, one of these masks includes circuitry that hardwires part of the operating system - a practice that leads to difficulties in standardisation which is discussed later (see section 4.3.4). There is no simple way to compare one card chip with another, as their description involves several parameters including power consumption, clock speed, memory size and types, geometric density, physical size, cost, robustness and security.

2.3.8 Cost and cost estimation

There are constraints on the technology that can be used in the manufacture of chips for smart cards, which are discussed later in section seven under the potential for improvement. New and cheaper methods of manufacture might affect the extent to which all concerned accept the cards, but the estimated cost of a card depends upon what economies of scale are anticipated, and what components are included in the estimate. The card is always part of a larger system that includes at least a reader and supporting software (Noakes-Fry, 1994, p. 204). According to Svigals, the value of the card itself is likely to be between US$2 and US$25 (Svigals, 1994, p. 112). An alternative estimate, from Lam, is from A$5 to A$40 (Lam & Low-Shang, 1994, p. 8). Neither of these figures includes the cost of readers or other supporting devices. The variance among these dated references shows the uncertainty at the time and the hopes that mass production would reduce costs. More recent figures in section 4.4.3 show that the reduction has been less than expected. Most authors claim that, like other electronic devices, the cost of smart cards will fall as a mass market develops, but others argue that it will not fall indefinitely because the demand for improved capabilities will outweigh the demand for lower prices (Haykin & Warner, 1988, p. 34). More detailed figures are given in the chapter four dealing with problems and difficulties.

2.3.9 Present day cards

To date almost all contact smart card applications use one of six chip families,

- Motorola 6805,
- Hitachi H8,
- Siemens SLE44xx,
- STMicroelectronics ST8 or ST16,
- OKI 627xx or
- Philips/Intel 8051.

Baker, in 1992, wrote of 30 types of chip but it is not clear what he regarded as a type (Baker, 1992). In 1994, a smart card had an 8-bit microprocessor working at 5MHz, and the memory available for all applications was seldom more than 8K. According to Zoreda, such limited capacity could be found in a PC 15 years earlier (Zoreda & Oton, 1994). In those 15 years, 64 bit, 166MHz microprocessors had become available and user memory was expressed in megabytes, but for the smart card chip there had been little change. Today a contact smart card used in an application typically has:

- a relatively slow 8-bit processor (5 to 14 MHz),

- RAM 256 bytes,
- ROM 8 to 20 Kbytes, and
- EPROM or EEPROM 8 Kbytes (Rankl & Effing, 1997, p. 49).

Duffy claims cards with 128 kbytes of RAM are made but it is not clear whether or not these are true smart cards (Duffy, 1994, p. 104). The chips used in contactless smart cards are, in all likelihood, proprietary extensions of chips designed for contact cards, but, for commercial reasons, details are seldom made public.

2.3.10 Conclusion

A reasonable conclusion from the foregoing is that whilst those smart cards now being used in applications have only limited memories and slow processors, more powerful cards are being developed by commercial concerns in secret and any investigation into their use should anticipate improvement. Some possibilities are set out in section seven of this chapter.

2.4 Biometric Identification Technology

2.4.1 Identification in general

It can be argued that good security begins with accountability which, in turn, depends on irrefutable, unfakeable identification. The argument, that unjustifiable identification is an invasion of privacy, is discussed later (see chapter four section nine). A person is identified by something they:

- have (a token),
- know (a password or PIN),
- are (a biometric feature), or
- can do (a signature or keystroke pattern).

(The term biometrics strictly related to the statistical analysis of biological phenomena and measurements, but has become widely accepted within the security profession to describe technologies used for personal identification (Sherman, 1992, p. 128)). A smart card can integrate two or three of these identifiers because it is a token and can respond to any of a password, a biometric feature, or some action.

2.4.2 Identification and verification

An identification system may be designed to establish an individual's identity by checking that his/her details are recorded in a database of many records, or merely verify that a claimed identity is correct. Identification systems are those in which it is necessary to prove either that the individual's details are in the database or that they are not. Both identification and verification can be illustrated diagrammatically. Identification is a much more demanding process than verification and either process might be necessary in vehicle management. For example, identification might be necessary to prove that an individual has a license (say at the time of a traffic violation) or has no license (say before issuing one) ("Best practice", 2000). Research to find improved methods of identification is being undertaken by authorities worldwide in law enforcement, health, welfare and other areas and the scope of the subject spreads beyond the focus of this thesis. As the main concern of this discussion is the case of a person seeking access to a vehicle, the complexities of identification have been left for others to investigate. Since any car is likely to have a limited number of drivers (a few dozen at the most), the vehicle-related applications for identification would be the identification of a driver, or a driver/vehicle pair. Returning to the verification process, an owner or driver seeking the use of a vehicle, and presenting a smart card together with a password, token or biometric feature, merely requires that the item (or, in the last case, the template extracted from the feature) be verified as being identical, or acceptably similar, to that on the card.

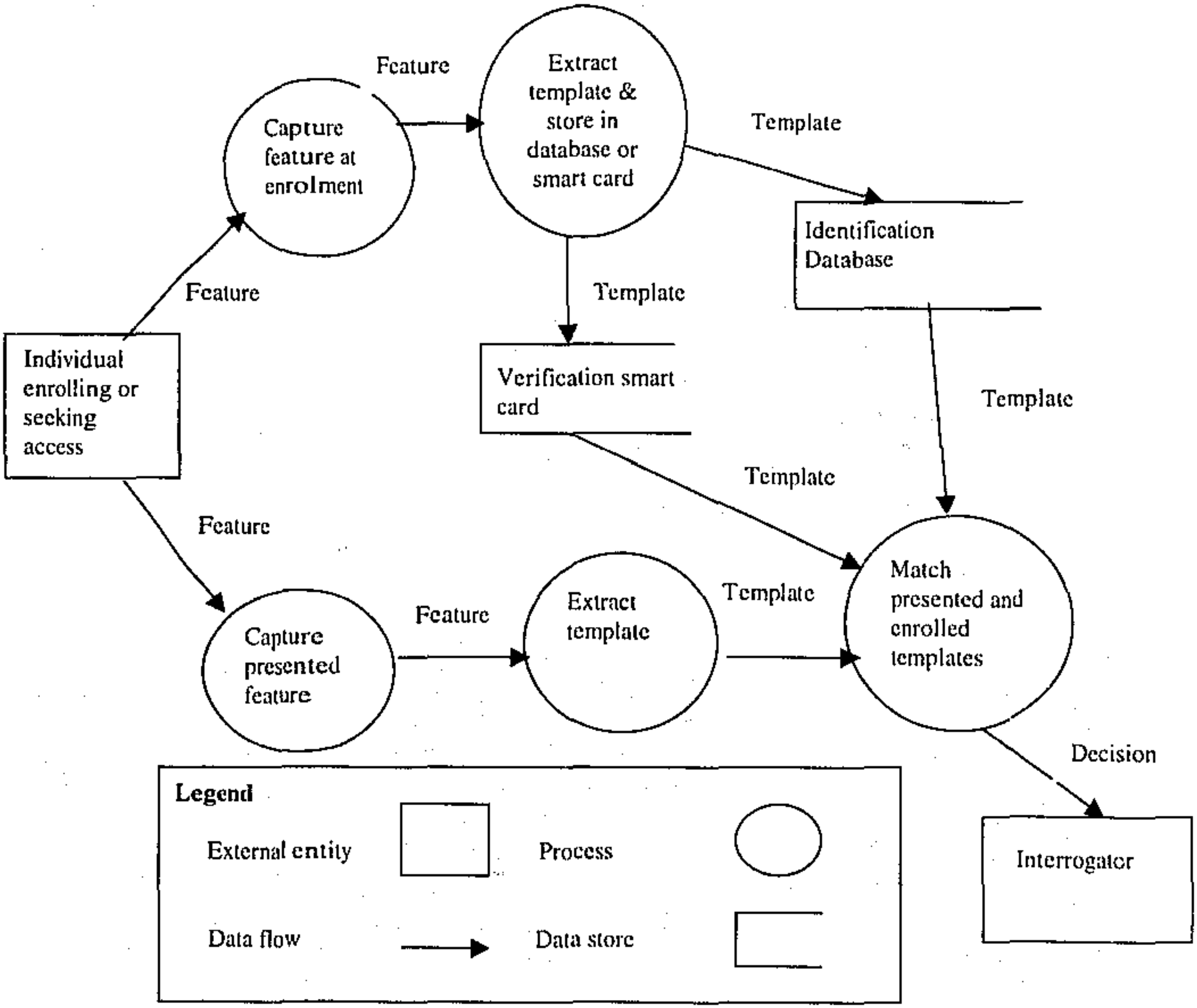


Figure 1 Validation and verification

2.4.3 Smart card identification

Authorisation is the process of determining that an entity may do what it seeks to do. A smart card authorisation system can be considered to have two aspects: user authorisation and card authentication. Both identification and verification may form part of user authorisation and have been discussed in the previous paragraph; but card authentication involves authenticating the smart card to the terminal. In the GSM cellular telephone system a symmetric challenge/response method is used because the reader is always on-line, but in off-line situations an asymmetric method is necessary. In the latter cases a challenge, provided by the terminal, is encrypted on the card using the issuer's private key and returned to the terminal, which decrypts it using the issuer's public key. In this way, at some cost in card computing resources, the terminal is assured that the card is a genuine issuer's card (Leach, J., 1995).

2.4.4 Biometric performance

Well known biometric features of individuals are fingerprints, retinal patterns, voice patterns and back-of-hand vein patterns, but there are others. Biometric techniques promise the best standard of user authentication, since they depend on something the owner is, rather than something he/she carries (and can lose), or something he/she knows (and can disclose). However, in the author's opinion, at least two weaknesses must be acknowledged, "comparison threshold" and "template vulnerability", described in the next two sections.

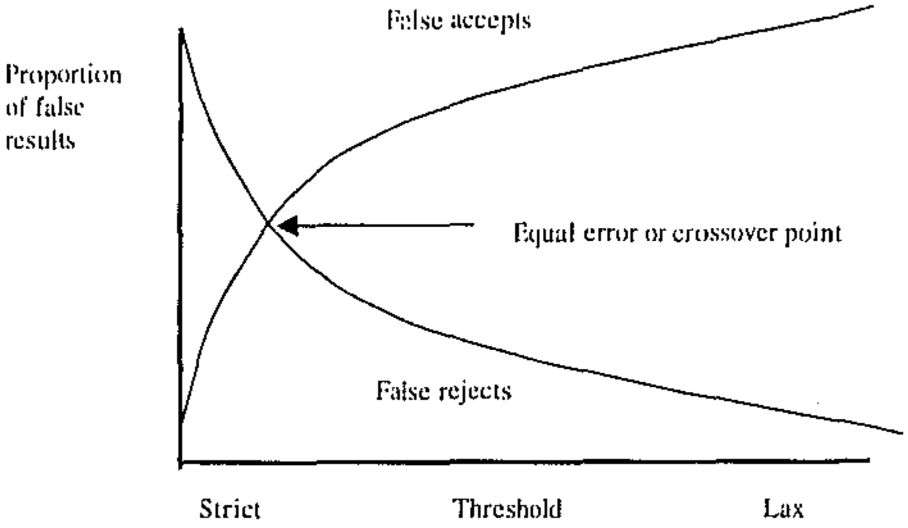


Figure 2: Receiver operating curves

2.4.5 Comparison threshold

The first weakness results because all the techniques involve a comparison of presented and recorded features (commonly images) and the two can never be identical but only similar to a greater or lesser degree. The required degree of similarity is known as the threshold. If a comparison detects a similarity better than the threshold it is termed a "hit". Occasionally a comparison will record a hit when it should not and fail to record a hit when it should: these results are termed false acceptances and false rejections respectively. If a graph is drawn with the values that could be chosen for the threshold along the abscissa and the proportion of false results as the ordinate, then receiver operating curves (ROC) can be plotted as in Figure 2. The need for an appropriate threshold is discussed in section 4.7.1 and the possibility of a variable threshold in section 7.3.6.

2.4.6 Template vulnerability

A second weakness in the promise of biometric techniques is that whilst "what we are" can be neither mislaid, nor stolen, and is difficult to counterfeit, the same cannot be said of a template (e.g., a bit string derived from an image of a human feature). The technique requires a scanner to be used to take an image of a biometric feature such as a fingerprint or back-of-hand vein pattern; and from this scan, it derives a template for storage on a smart card and, possibly, in a database of authorised templates. If the template was captured by a rogue terminal and written by a fraudster onto a counterfeit card, the counterfeit could then masquerade as a legitimate item, unless asymmetric card authentication is also used.

2.4.7 Biometric features

Of human identifying features, the fingerprint is the best known, whilst the voiceprint is the cheapest, and the retinal pattern the most expensive, to capture. There are a number of others including the "back-of-hand" vein pattern. These four features each represent a possibility for use in vehicle management, and are now considered in more detail.

2.4.8 Fingerprint

Fingerprints are usually processed in one of four ways: specifically,

- capturing the image optically and then converting it to digital form;

- capturing the image directly into digital form using capacitive sensing ("UniBO Fingerprint Capacitive Sensor", 1997);
- sensing the heat differences between the ridges and valleys of a fingerprint and then converting the gradients to digital form: an approach being developed by a French company, Thompson-CSF (May, 1998),
- capturing the image optically and then processing it with an optical computer, without digital conversion. It is claimed that, with this method, the work is done using parallel processing and is fast ("Mytec Technologies: Technology", 1996, May 13).

Following this processing, in most systems a template is derived. As yet none of the last three alternatives has an established track record in industry. Of the several human features that can be used in biometric identification, there is a wealth of experience only in fingerprint collection and use (Ruggles, 1998). Fingerprints are almost certainly unique to each individual, their capture is non-invasive, and a scanner could be designed to collect fingerprints without being exposed to either the weather or casual attack. The genetic process by which fingerprints are generated is believed to be random, since, so far as is known, those of relations, even identical twins, are not similar. However, because of its association with crime, the technique may not be acceptable to the public (Millar, 1994).

2.4.9 Voiceprint

Another identifying feature is the voiceprint, which is commonly used because the captured pattern and the recorded template are more easily compared. However voiceprints are probably less reliable than the fingerprints, in that both the false acceptance rate (FAR) and the false rejection rate (FRR) are higher (Ruggles, 1998). Furthermore, it may be difficult to mount a microphone inside a vehicle (out of the weather and vandal proof) and still be able to capture the voice pattern.

2.4.10 Eye retina

Retinal patterns are known to be unique, but the scanning and matching techniques are expensive, thought to be regarded by the public as invasive, and may provoke antagonism amongst people who are sensitive about their eyes (Miller, 1994).

2.4.11 Back of the hand

The back of hand vein pattern has been investigated because it does not have the stigma of a fingerprint and because the image/template comparison may be a little simpler. A disadvantage is that vein patterns are not so certainly unique as fingerprints (Mehnert, Cross & Smith, 1994) and require either a rather large scanner external to the vehicle, or a fist-sized hole in a panel.

2.4.12 Comparison chart

The chart in Figure 3 provides a simplified but visually convenient display of the relative merits and shortcomings of the features mentioned above. Symbols for meritorious features are placed towards the periphery of the chart, but this positioning is only the author's current interpretation of the descriptions provided in the references, and has no mathematical validity. Other writers may evaluate the features differently.

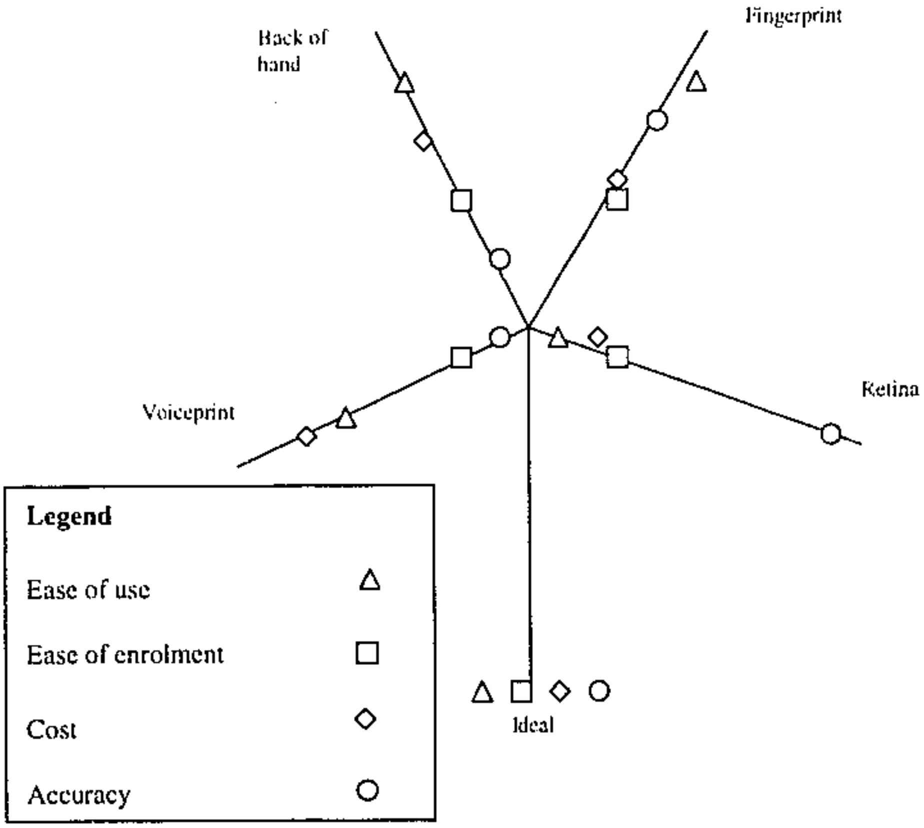


Figure 3 Visual indication of biometric system merits

2.4.13 Scanners

An optical scanner may be used to capture the image of a biometric feature such as a face, back-of-hand vein pattern, or in one system, a fingerprint. At present, commercially available optical scanners use Charge Coupled Devices (CCDs) and occupy a volume between 250 and 1000cc. Scanners are expensive now but, according to Dan Maase, vice-president at Identix, like other electronic devices, they can be expected to improve in performance and fall in size and cost (Abate, 1997). The optical types usually employ technology similar to that found in a digital camera and can capture images in both the visual and the infrared portions of the electromagnetic spectrum. The aforementioned alternative fingerprint scanner, based on capacitive sensing, although now being marketed in at least one model, is still being investigated; but it may have advantages in both size and cost (Abate, 1997). Generally, each of the biometric identifiers requires a different type of scanner. At present retinal scanners are the most expensive and "back of hand" scanners the cheapest, whilst fingerprint scanners fall in between, ranging in price from US$100 to US$1000 (Miller, 1994).

2.4.14 Pattern recognition

Having captured the image, its pattern must be recognised, a process defined as the identification of images by their shapes, forms, outlines or other attributes (Weik, 1989). In biometric identification, two or more images may be compared, or a template extracted and compared to other stored templates, to determine similarities or differences. The following sequence of steps may be required.

1. Preprocessing which may include enhancement, segmentation, skeletonization and smoothing. Briefly,
   - enhancement seeks to remove noise, especially the background to the image,
   - segmentation, or thresholding, seeks to convert a grey scale image in which features have fuzzy edges to one in black and white (a binary image),
   - skeletonization, or thinning, is used to reduce all lines to a common width, since the pattern of an image rarely depends on the thickness of the lines with which it is drawn

- smoothing, usually directional smoothing, and/or filtering is used to remove anomalies, or spikes, that may be introduced during skeletonization (Mehnert, Cross & Smith, 1994).

2. Feature extraction which identifies significant items, or features and ignores redundant data (Ratha, Chen and Jain, 1995).
3. Image registration, which is concerned with variations. Inevitably images are not captured at the same time, with a single sensor, from one viewpoint and, consequently, there are always variations which can be any of three types:
   - misalignment due to the acquisition method,
   - variations due to intensity or perspective, and
   - variations that are of interest.

   Image registration seeks to eliminate or identify the first two variations (Gotlesfeld-Brown, 1992, p. 325).
4. The derivation and storage of a template or bit-string representation of the significant items of the image.

In the process of biometric verification smart cards could have any of three roles. They could:

- merely store and make available the template derived from the feature of the enrolled person, or
- perform as above, but in addition, compare the stored template to the template of the supplied image which has been derived elsewhere, or
- derive the template from the supplied image and compare it to the stored image.

Only the first role has been implemented. In the author's opinion, the restriction to the first role is probably because the work of pattern recognition and comparison is computationally intensive and, as yet, beyond the processing capability of any smart card used in a major application.

2.4.15 Conclusion

From both management and usage viewpoints there is a need to verify drivers' identities and authenticate them to the vehicle they drive. Fleet managers and traffic authorities need to know beyond dispute who is driving a vehicle at critical moments, whilst the average owner will wish to deny others access to what is his/her second most valuable asset (after a house). The possible further need for authorities to validate applicants for licenses and, perhaps, identify drivers suspected of offences, requires more demanding processing but, even so, biometric identification might be used in this area. Whilst biometric technology promises an eventual high standard of identification, as yet it has weaknesses and requires unacceptably substantial computational resources. If, eventually, these drawbacks are overcome, fingerprints are likely to be the chosen feature. However, as a technology, it may always be suspect because of the miniscule, but undeniable, uncertainty of comparisons and, paradoxically, the more nearly infallible it becomes the more vociferous will be the protests of those who believe identification to be an invasion of privacy. Until, if ever, public opinion matures to the point where identification is accepted and widely used, cost and unfamiliarity are likely to render biometric methods unpopular, even in what is merely a niche application.

2.5 Transponders and access tokens

2.5.1 Description

An alternative to identifying people by personal features is to equip them with transponders (small versions are called tags) as access tokens. The difficulty of using biometric features to identify individuals, and the present cost of scanners could be by-passed by equipping authorised individuals with one of these devices, which would respond to a radio frequency challenges from within the vehicle with a unique bit-string signal in order to authorise access. The possibility of identification in this way might be facilitated if the Bluetooth communication specification was widely adopted ("Short description", Nov 2000). (Note: A contactless smart card can be thought of as a sophisticated transponder, since current versions are capable of on-card processing before responding with a signal.) Although a transponder could be counterfeited, or the owner could lose it, or be robbed of it, modern tags are small and could, for example, be incorporated into something, such as a watchstrap, that rarely leaves the owner's body. Furthermore, after gaining access to the vehicle using the tag, the driver could be required to enter a PIN at a keypad. A thief who either stole the tag, or simply forced entry to the vehicle, would still have to overcome the need to supply the PIN before moving off. A secondary advantage is that transponders located in the vehicle can be used as tracking beacons as well as for identification. Owners of valuable animals, such as stud animals, sometimes improve their protection against theft and the probability of recovery, by attaching a transponder to the creature: often by inserting a tag under the skin. Heavy haulage carriers, both rail and road types, also use these devices to keep track of containers and wagons: therefore, as the transceivers that communicate with the transponders become more common, it is possible that fitting them to vehicles will increase the chance of recovering those stolen.

2.5.2 Vehicle tracking application

A paper presented to a colloquium on vehicle security in Britain in 1993 proposed a system based on this idea of tracking beacons and Geason describes a similar system, the Massachusetts Lojack System (Geason & Wilson, 1990, p. 32). The Lojack system appears to be a commercial success because, despite the obvious drawback of its high cost, now (admittedly almost ten years after its first launch) it is used in 12 US states, in Moscow and in South Africa - all high-risk areas for car theft. A less widely known system, QuikTrak, briefly described in section 3.5.6, is marketed in Australia, but has not achieved general popularity. However, Homel, apparently considering car theft from a social rather than technical point of view, quotes Clarke and Harris (1992) as considering tracking devices may merely change the target, but do not significantly deter thieves (Homel, 1994).

2.5.3 Disadvantages

The social aspects will not be considered here, but technical drawbacks in using transponders, either as tracking beacons or as access tokens, must be acknowledged.

- The response of a transponder can rarely be detected through metal, a factor which limits the possible locations for this type of beacon in a vehicle.
- A reasonably competent technician with the necessary equipment could easily scan an item for any affixed transponders.
- To be effective and justify police effort, a high proportion of vehicle owners would have to participate, and probably neither they nor the insurance companies would be prepared to meet the cost.

The possibility of facilitating tracking using smart cards is discussed in section 3.5.6.

2.5.4 A different system

A somewhat different access token system, named Vehicle Anti-theft System (VATS), developed by General Motors used a small resistor pellet embedded in the ignition key. The pellet had a specific electrical resistance, like an electrical code. Installed elsewhere, in a hidden and inaccessible part of the vehicle, was a decoder with a complementary resistance. When the key was turned in the ignition lock the car would start only if the decoder's resistance and the key's resistance matched (Biles & Willing, 1987, p. 50). Nevertheless, the system does not seem to have been widely used.

2.6 Passwords and PINs

Passwords, of which PINs are a sub-set, are an ancient technique for identification, and their drawbacks are well known (Lynch, 1998). If the same password is used by more than one person and is disclosed, responsibility for its disclosure is difficult to determine. Another problem is that if passwords are changed frequently, memorising the correct password can be a chore, so, to relieve the strain on memory, the passwords are too often written down. Obviously the practice of recording a script copy seriously degrades the protection they afford: therefore, to make recall easier, authorised persons are sometimes permitted to choose their own passwords. Sadly, studies have shown that password guessing is more likely to succeed when holders are allowed to choose (Fak, 1991).

2.7 Potential for Improved Smart cards

2.7.1 Design constraints

The engine of any smart card is its chip; therefore the potential enhancement of the card is heavily dependent upon chip improvement, which in turn is constrained because the card's chip requires unique features that militate against the use of some leading edge chip technology.

- Probably most importantly, to reach a mass market, chips must be cheap, which requires high volume production, and this precludes some of the more exquisite manufacturing techniques (Fancher, 1997).
- Furthermore, in many applications, smart card chips must be reliable and, hence, tend to exploit only proven technology (Rankl & Effing, 1997).

- In addition to being cheap and reliable, the chip must be small enough so that the card may flex normally, be thinner than the card and no bigger (and preferably smaller) than 5mm by 5mm (Daniels, 1995).
- The chips may not draw much power, because of the problem of disposing of the resulting heat, and must work even when dirty (Owen, 1995).
- Generally, financial institutions consider that the chip component should be a single chip, or separate unconnected chips, and not a cooperating multiple, because multiple chips would need connections that would be vulnerable to hacking and to damage through card flexure (Paterson, 1991; Owen, 1995).
- Since it has power only when in or near a reader, the chip data memory must be non-volatile, be capable of being rewritten many thousands of times, and be readable for several years.
- Finally, a smart card chip must be extremely resistant to any attack on its security, must be virtually impossible to counterfeit and, like a patriotic spy with a cyanide capsule, must self-destruct rather than divulge its secrets. Although smart card chips approach this security ideal, it is likely that, given sufficient resources (well into the millions of dollars) and world-level expertise, they could be "cracked" (Anderson & Kuhn, 1996).

In short, the makers of smart card chips are faced with a challenging requirement.

2.7.2 Leading manufacturers and products

Technical detail about the chips used in smart cards is seldom released to the public. However, in 1997 each of four major manufacturers gave some information about a chip incorporating a cryptographic co-processor, and each claimed their product was the most suitable for smart card installation. The incorporated crypto-controller circuitry accelerates public key encryption, and is a hardwired part of the ROM; a feature that suggests financial institutions were the target market. The available information is set out below and summarised in Table 1.

- In March, Motorola published details of a new chip, claiming it to be the fastest of its kind ("Motorola", 1997). The RAM and ROM of this crypto chip are greater than that of most card chips, but the EEPROM is only half that of some others.
- Hitachi, also in March, announced the "launch" of a 16/8-bit card chip, the H8/3109, a version of the H8 family specifically customised for Mondex cards. (Mondex, owned and sponsored by MasterCard, is a major potential electronic purse card issuer). The meaning of the term 16/8 was not explained by Hitachi, but possibly indicates that processing, and data transfer and storage, employ different word sizes, one being 8-bit and the other 16-bit. Hitachi does not list a sheet for the H8/3109 amongst the data sheets that are published on its web site.
- In August, Siemens promulgated some information about a chip designed for smart cards, the SLE 44CR80S, which was also, promoted as a high-security chip and, therefore, presumably intended for financial sector applications. The statement particularly stressed the chip's small size, given as 15mm^2 (Hochholzer, 1997).
- In October, 1997, at Cartes '97, Philips, a smaller manufacturer, introduced the MIFARE.PRO a dual interface card chip family, based on the long established Intel 8051 chip. The chip can be accessed both remotely, and through contacts,

but, at present, uses symmetric encryption. Philips says that, eventually, the chip will be the more powerful "combi" SmartXA, discussed shortly, and will incorporate a FAMEX crypto-coprocessor enabling asymmetric encryption (MIFARE.PRO", 1997).

None of the announcements gave the clock speed, which is likely to be the normal 5MHz used in chip cards. MasterCard selected the Hitachi chip for its Mondex electronic purse and Visa the Motorola and Siemens designs for its Visa-Cash alternative. As yet neither purse scheme has a major application. Although the MIFARE.PRO chip is at present being touted as most suitable for public transport ticketing, the promised crypto-coprocessor suggests that Philips has an eye on the potential market for a financial application. Apparently, the major chipmakers believe that an enhanced crypto-chip with limited RAM and large ROM is what the financial market requires, but so far, the institutions themselves have established only pilot schemes. However, multiple applications require large EEPROM or other rewritable memory.

Table 1. Prominent smart card chips

Manufacturer	**Product No**	**RAM (bytes)**	**ROM (kilobytes)**	**EEPROM (kilobytes)**	**Bits**
Motorola	M68HC05SC49A	896	20	4	8
Hitachi	H8/3109	256	14	8	16/8
Siemens	SLE 44CR80S	256	17	8	8
Philips	MIFARE.PRO with 80C51 dual interface	256	20	8	8 *

* Eventually MIFARE.PRO is to have the 16-bit SmartXA chip.

2.7.3 Basic or "no frills" designs.

If a less sophisticated chip was acceptable, it might be possible to reduce card costs. Probably with that in mind, French researchers have designed a smart card chip for limited payment systems (SCALPS). The researchers merged the processor and coprocessor on a small chip dedicated to public-key cryptography, added parts needed to obtain a low-cost smart card and claim to have drastically reduced complexity without affecting the chip's usefulness (Dhem, Veithen & Quisquater, 1996). Toshiba also claims to have a "no-frills" chip and estimates that prices will drop below 200 yen, or US$2.00, per card with the introduction of its CZ-3018 card. Toshiba says the new card has a chip with an 8-bit CPU, 6K of ROM and 128 bytes of RAM, supports enhanced data security and meets both the standard ISO/IEC 7816 and EMV standards. The lower costs are primarily achieved by downsizing the memory capacity ("Toshiba introduces", 1996). So far there are no reports of commercial organisations seeking to exploit either the French or the Japanese, proposal.

2.7.4 A "de-luxe" design

It may be technically feasible to increase both the speed and the memory of smart card chips. The European Chip Architecture for SmartCArds and secure portable DEvices (CASCADE) project, part of the European Strategy for Promotion of Research in Information Technology (ESPRIT) Open Microprocessor Initiative

(OMI) initiative, seeks to develop a Reduced Instruction Set Computing (RISC) chip with a 32-bit architecture, 32K of non-volatile memory and a clock speed of 20MHz. The project was launched in 1993 as a cooperative effort between French companies (Gemplus and Dassault), British companies (Advanced RISC Machines (ARM) and Domain Dynamics) and a number of universities. The stated aims of the project were to achieve:

- more programmability for shorter time-to-market and greater versatility,
- better configurability with multiple applications at the user's will,
- an ability to handle the unscrambling of real-time audio-visual data of consumer entertainment applications, and the
- ability to support enhanced human-card interfaces such as voice control (Peyret, P., 1994).

More technically, the designers claim:

- non-volatile memory life of 10 years,
- clock speed of 20MHz,
- more memory in "flash" technology,
- a 32-bit word,
- a lower power requirement (1.8V), and
- RISC technology.

In a March 1997 press release, Gemplus said that Texas Instruments would be manufacturing the chip in 1998 ("Cascade a new chip", 1997). However, there are still no reports of any commercial application and Motorola, one of the dominant chip manufacturers of smart card chips, spent large sums to up-grade its facilities for producing the usual 8-bit chips ("Motorola, 1997). (Note: In May 1999, Atmel purchased the Motorola Smart Information Transfer (SIT) division that manufactures the M68HC50SC49A.) A reasonable conclusion is that although a more powerful smart card chip may be technically feasible, commercial factors are likely to delay its introduction for some time yet.

2.7.5 Contactless card potential

Contactless smart cards, unlike contact versions, will probably find their main market in rapid access, rather than financial, applications. Therefore, in addition to memory size, significant parameters are reading distance and data transfer rate, but security may be relatively less important.

2.7.6 Memory size

A limitation of the devices is that they necessarily have smaller memories than contact versions, due to the need to provide space on the silicon for additional circuitry such as coils, capacitors and charge pumps, but the situation might improve. Motorola, in a joint venture with Matsushita, is developing a new contactless card memory called Y1 (Fox, 1995, p. 22). Y1 is one of the perovskites (strontium bismuth tantalate) a material similar to some used in high temperature super-conductors. A chip using Y1 might have a rewritable memory up to 100 times greater than one using standard silicon dioxide, and a life with a greatly extended number of rewrite cycles (Johnstone, 1998, p. 38). The technology is also known as ferroelectric memory or FRAM.

2.7.7 Reading distance

Another contactless card problem is uncertainty about the maximum reading distance, as can be seen from the following estimates. Although the range may seem to be increasing this may not necessarily be true as the different distances are achieved with different technologies and frequencies.

- 3mm -10mm ("Smart Card Technology", 1994)
- 10cm (Duffy, 1996),
- metre (Owen, R., 1995),
- metres (Johnstone, 1998).

A different author, Rankl, gives the following distances:

•	capacitive coupling		1mm,
•	inductive coupling	- reading	1 metre,
•		- writing	10cm (Rankl & Effing, 1997).

The cards used by ERG in the HongKong ticketing project, described in section 2.7.9, use inductive coupling. An advantage of "close-coupled" cards is that they are subject to less wear than contact cards and the reader is less vulnerable to vandalism but the need for near contact would probably mean that they have no application in public transport ticketing.

2.7.8 Data transfer rates

The high frequencies used mean that high data transfer rates can be achieved and can vary over the entire range (9.6 to 76.8 Kbaud) specified for contact cards by ISO

7816. Proximity cards use higher frequencies (13.56MHz) than vicinity cards (125KHz) and, data transfer rates, therefore, vary from over 100 Kbytes/sec to about ten. Both performances lie within the range specified by standard ISO 14443. Two specific estimates of the contactless card data transfer rates follow.

- 19.2 Kbytes/ sec (Owen, R., 1995) and
- 106 Kbytes/sec (Duffy, 1996).

As can be seen, the information is dated and the current situation is probably rather better. A data transfer rate of 100Kbytes/sec results in a ticketing process of about a tenth of a second.

2.7.9 Dual chip cards.

In HongKong, Gemplus has devised a dual-chip card. The technology provided by Gemplus incorporates the latest technology in smart card usage, and the application is a result of a joint effort by City University and Hang Seng Bank. Technically, the card is fabricated with both contactless and contact chips, with the contactless chip supporting the access applications and the contact chip supporting the stored-value function ("Banks launch", 1997). Apparently the two chips are not connected, thus maintaining security at the cost of some foregone flexibility in application design.

2.7.10 Combi/Dual Interface cards

Many contactless card applications, usually in transportation, use a dual interface card in which the microprocessor can be accessed either through contact or remotely.

Software usually conforms to the MIFARE architectural platform developed by Philips and the chip is often an Intel 8051, produced by Philips, presumably under licence. The arrangement results in a rather power hungry device with relatively short-range access. Since 1998, Philips has been advertising a SmartXA 16-bit chip with 4k RAM, up to 32k ROM and up to 32k EEPROM. The chip has a crypto co-processor and Philips claim it can handle asymmetric encryption with up to 2048-bit keys. Security is said to be maintained through the use of hardwired firewalls (Mifare News, 1997-10-01).

2.7.11 Other potential advances

Other potential smart card hardware advances may be achieved. Possibilities are:

- improved geometric density,
- more powerful coprocessors,
- improved plastic card manufacture,
- improved chip embedding,
- new memory storage materials.

The last three possibilities deserve rather more detail. Currently the plastic used in card manufacture is either Acrylonitrile Butadiene Styrene (ABS) or Polyvinyl Chloride (PVC). ABS, which involves injection moulding, is more durable and cheaper for small production runs, but cannot have a magnetic stripe added. PVC, which is laminated, is cheaper for large quantities and is easier to emboss but has a shorter lifespan, less resistance to extremes of temperature and presents a hazard for the environment. Printing on ABS has made progress in the last few years, which is an important consideration because it is hoped that advertising will pay for the cards (Benhammou, 1997). Other materials have been tried but so far have proved too costly. There are now proposals to embed the chip with a metal lead frame around it to protect it from flexure of the card (Benhammou, 1997), and use new yttrium and ferroelectric materials mentioned earlier.

2.7.12 More compact rewritable memory

Initially, because space on a smart card chip is critical and ROM requires only one quarter of the space required by EEPROM, most card operating systems were created using a ROM mask, one of the chips manufacturing masks. The operating systems were thus hardwired (see section 4.3.4) and usually optimised for a specific application or applications; a technique that resulted in a robust, secure system, but made the use of the one card for various applications, let alone the creation of a multi-application card, very difficult, if not impossible. The space constraint still applies, but there is now a tendency to store part of the system code in EEPROM. Hopefully the use of non-volatile, rewritable memory- may lead to a successful multi-application card (see section 7.3.4).

2.8 Conclusions

As already noted, at present smart cards have limited memories and slow processors, but eventually a design that is capable of the authentication, stored-value functions and portable record keeping that is required for vehicle management, will be devised. However, a discussion of whether and how such a card might capture the necessary mass market, and a detailed analysis to determine what capacity and performance must be achieved, is deferred until chapters five and six. The best identification concept amongst the new technologies may be the combination of smart cards with biometrics, but although improved smart cards will probably continue to be designed and manufactured, whether any biometric method of identification will achieve a universally acceptable standard of performance is less certain. Nevertheless, at present, a smart card system seems to be the most promising possibility for personalising an equipment or device to a specific user (Noakes-Fry, 1994, p. 202). In particular, if the system could capture the template of a user's identifying feature to a smart card during an enrolment process and compare it with a supplied template derived from a scanned image, then, if the two templates match, positive identification would have been achieved. Alternatively the user might be required to supply a PIN which the smart card could compare to a previously stored item and then, given a match, send a code to a decoder that would then, and only then, activate the equipment or device. Therefore, referring back to the major applications of a smart card as reported by the New Zealand Futures Trust, (Butler, 1996) identification followed by coded activation promises to provide the personalised, extendible authentication that is required, whilst there are no apparent technical impediments to eventually storing value and maintaining necessary vehicle management records.

3 SMART CARDS & VEHICLE MANAGEMENT

3.1 Introduction

Chapter one identifies the components of vehicle management as traffic management, usage control, maintenance and security, and chapter two considers the current state and the potential for improvement, of smart cards, biometrics and other relevant technologies. Continuing to employ the sequence introduced in chapter one, the present chapter examines how the aforementioned technologies might be applied to improve management of each of the listed components, and mentions the additional driver convenience that might be achieved as a by-product. The approach involves dealing with each identified aspect in turn, but traffic management and vehicle security deserve the most attention because, as will be seen, in both cases controversial matters must be addressed. The controversies arise because the four main groups concerned with vehicle management (authorities, fleet owners, owner-drivers and drivers) do not have completely identical interests and are unlikely all to favour the same management solution. Therefore, an attempt is made to take a balanced view and, when considering how the technologies might be applied to the management problem, to identify advantages that might be attractive to each group.

3.2 Traffic Management

3.2.1 General

As defined in section 1.2.1, traffic management involves observing and influencing the behaviour of motorists (an activity in which identification is usually essential) and rapidly recording events (a task suggesting a degree of automation). Smart cards could facilitate several parts of this process: in particular,

- monitoring behaviour,
- obtaining the facts relating to accidents and other incidents, and
- collecting fees, charges and penalties.

These points and a few subsidiary matters are now considered

3.2.2 Behaviour monitoring

One day, if the mounting road death toll or the selfish and irresponsible behaviour of a few motorists becomes unacceptable to the electorate, control of road traffic might approach the tight regulation imposed on air traffic. Whilst control is unlikely to reach the point where drivers must file the equivalent of a flight plan before commencing a journey, it is not inconceivable, in urban areas, that vehicles be fitted with the equivalent of an identifying beacon and be subject to individual or group direction regarding speeds, diversions and "special charge" or exclusion zones. The technology is already used on buses in Brisbane. If smart card systems ever became normal in vehicles, the authorities responsible for monitoring and enforcing traffic, pollution, and congestion regulations, could make use of them. The card could be part of a basic system, analogous to aircraft radar logging and cockpit voice recording, and could provide a simple "black box". Similar technology to that used for road pricing could be used to interrogate vehicles as to the driver's licence details and speed - but motorists might not be enthusiastic.

On a less futuristic note, even if remote interrogation facilities were not available, a traffic officer equipped with a suitable reader could obtain at electronic speeds those details that, at present, are laboriously recorded with a ball-point pen. The concept of a smart card drivers' license is not new. A Swedish invention, the "kittelock", already implements it and has been recommended for an ESPRIT award, (Stott, R., 1995). In Austria, in another application of the concept, a multiple application card issued by Kapsch, an Austrian telecommunication company, stores details of the motorist's license and insurance cover, and acts as a token to unlock the doors (Duffy, 1996). Finally, in the USA, the National Committee for Information Technology Standards (NCITS), formerly the ANSI, has produced a draft standard for a smart card driver's licence, but, so far, there seem to have been no implementations ("Driver's license", 1999).

Given an on-board smart card system, the automatic identification of both vehicles and drivers would be possible, and data that were collected automatically could be analysed in real-time to determine traffic conditions at selected times and places. Extensions to the system might be possible: e.g., if the smart card incorporated an electronic purse application, a fee could be extracted from any vehicle entering a designated congestion control area. Furthermore, if the card was mounted in a transceiver, it is even possible that, in reciprocal communications, drivers could be advised of traffic conditions ahead of their presumed route, and diversions recommended. Harrop lists a number of trials and initiatives of this nature undertaken in the US, Europe and Japan (Harrop, P., 1993, pp.110-112).

3.2.3 Black box

Ascertaining the facts concerning actions prior to, and at the time of, an accident can often be difficult. Wigan, quoting "IVHS America (1994) IVHS Crash data needs" (a report of the Intelligent Vehicle Highway System (IVHS) America project), writes,

> "An onboard 'black box' recorder would be an invaluable legal and enforcement resource. If such systems are designed to record even the last 100 seconds before a collision, then identification and privacy issues can arise. If such systems are designed to record continuously and especially if they were to transmit data for central storage and analysis, then a substantial surveillance pattern emerges." (Wigan, M., 1994).

That may be so, but the 'black box' might also allow blameless drivers to prove their innocence.

3.2.4 Road fee collection

Smart cards could be part of a more general, automatic, "road fee" collecting system. An experiment by the Transport Operations Research Group of the University of

Newcastle on Tyne, in Automatic Debiting and Electronic Payment for Transport (ADEPT), has developed a new generation of road-use pricing. The experimental technology incorporated an 'intelligent' communications transponder and smart card in the vehicle for automatic non-stop payment (Blythe, Burdon, Clark, Givens & Rourke, 1994). Results of an ADEPT experiment at Cambridge are claimed to have proved that road pricing is technically feasible, although some problems remain, mainly relating to "multi-lane enforcement, the performance and security of smart cards and the operational issues surrounding integrated payment" (Blythe, Clark & Rourke, 1994, p.45). However, other authors are less optimistic: for example, Harrop writes, "These and other challenges will provide a recession-proof source of employment for the talents of many electronics engineers for years to come." (Harrop, P., 1994). Furthermore, Clark states, "What is certain is that it is a debate we will hear more of over the next few years." (Clark, J., 1994). Four years later, in September 1998, under the special conditions that apply on the small island state of Singapore, an electronic road pricing (ERP) system was installed on three highways and at entries to the central business district ("More about ERP", 2000). It replaced an Area Licensing Scheme (ALS) covering the central business district and a Road Pricing Scheme (RPS) implemented on the island's three main expressways: both schemes were manual and had been found to be cumbersome, labour-intensive and inflexible. The ERP uses a smart card installed in a special in-vehicle unit that communicates with toll stations by radio and incorporates an electronic purse issued by NETS, a consortium of Singapore banks. Worldwide, Certified Wide Area Road Use Monitoring (CWARUM), a more far-reaching and futuristic scheme, is under discussion (Malik, 1998). Clearly, road pricing is under consideration by many national and regional governments, but a more detailed examination of how smart cards might be used to facilitate it, is left for future study.

3.2.5 Parking fee collection

The use of electronic purse smart cards as a way to pay parking fees has the usual advantages of cashless payment; in particular, avoiding the threat of vandalism of, and theft from, coin meters. In addition, purse use could enable authorities to accumulate statistics that would be of value in planning; however, two major prerequisites are:

- the widespread adoption of card purses, and
- standardisation (preferably international) of the technology for parking fee collection.

Trials using both contact and contactless cards have proved the technical feasibility of the proposal (Luk, J.Y.K., 1995)

3.2.6 Pollution and congestion control

Civic authorities are becoming increasingly concerned about pollution in urban, and especially central business district, areas. Pollution from wood or coal fires is more obvious, but the carbon monoxide and nitrous oxides from poorly tuned vehicles are more toxic (Ponneah, 1998). Sensors to determine the lambda, or air/fuel ratio, are already fitted to modern vehicles (Hillier, V.A.W., 1988), and their readings might be recorded on an "in-vehicle" smart card. At present, there is no external monitoring of sensor readings, but, given a smart card system that was politically acceptable to the electorate, authorities could interrogate vehicles remotely and ascertain the recorded toxicity level in the same way as licence and registration numbers might be obtained (see diagrams 3 and 4).

3.2.7 Vehicle related purchases

Automated payment for many purposes might be unpopular but could also have desirable aspects for the motorist. Automatic electronic fuel vending systems are already installed at the depots of some major closed fleets (Arazi, 1991, p. 648), and one can speculate that automated car washing is likely to follow. As mentioned in chapter one, about one in 10 vehicles is a fleet vehicle and, although no data has been collected, it is not inconceivable that, collectively, they could travel as much as half of all road miles travelled. Currently, petrol stations have the capability to record data for fleet owners and are increasingly under pressure to accept payment by both credit and debit cards; a method of payment that requires expensive, on-line authentication of many different cards, for what are usually relatively small, low-margin sales. A smart card incorporating an electronic purse provides an attractive option from the point of view of the retailer (Dick, D., 1995). Perhaps, one day, the driver will be able to open the fuel tank filler from within the vehicle, pay either with a contactless card or by placing a contact card in an adjacent reader, and have the tank filled by a robot arm ("Robot", 1997).

3.3 Usage Control

3.3.1 Journey records and vehicle handling

Usage control is more likely to be favoured by owners than by authorities and drivers. Fleet vehicle drivers are customarily required to keep a record of their journeys, and, by recording the odometer reading and time of each start, a smart card supported vehicle logger would facilitate the chore; particularly if, by way of a keypad, a code number could be entered simultaneously to indicate the trip's purpose. The maximum deceleration (indicating an emergency) or maximum speed between vehicle activations could also be recorded and, since the smart card would probably be personalised, there would seldom be uncertainty about who was the driver. These features might bring a significant improvement in recording of fleet vehicle usage, because, although they have been on the market for some years, automatic vehicle loggers have been too expensive for most applications. Basic versions, with limited recording capability, start at about A$750; more comprehensive, but still limited, versions cost A$1500 or more; very expensive loggers can record vehicle handling techniques such as gear changing or driver alertness; and, no known version accepts input from the driver. Nevertheless, whilst fleet managers might welcome a cheaper alternative, employed drivers might resist their introduction (Wigan, M., 1994). Owner-drivers might accept the envisaged systems if they were not too expensive and privacy was maintained, but it is arguable that little would be gained by their use. The reaction of a small sample of fleet managers is discussed in section 7.8

3.4 Maintenance

If vehicles had suitable interactive readers, service mechanics could record the completion of maintenance activities, such as oil or tyre changes, on a vehicle's smart card, and the card could then be programmed to display in-vehicle reminders when servicing was due. Drivers could also use a card system to record faults or suspicious symptoms as they were observed; thus, to some extent, relieving themselves of the need to make a report at the end of the journey. In section 1.2.3 the possibility has already been mentioned that, in vehicles fitted with OBD, faults that are diagnosed automatically could be recorded automatically on an installed smart card. With automatic fault recording, the validity of claims for repair under warranty might be more easily established, leading to reductions in fraudulent claims and extension of warranty periods.

3.5 Vehicle Security

3.5.1 General

Security is the aspect of vehicle management likely to be of most interest to owner-drivers, because vehicle theft is common in modern society, but, as mentioned in section 1.2.4, a discussion of vehicle theft has been relegated to Appendix 3. There seems to be a consensus amongst criminologists that approaches to deterrence focusing upon detection, arrest and conviction are unlikely to be effective (Homel, 1994). Instead, the manufacture of more secure vehicles and other target hardening strategies are advocated (Clark & Harris, 1992). Accordingly, after a brief mention of standards, which list a number of security precautions, those precautions will each, in turn, be outlined: an approach which should not be taken as an indication that the criminologists' view is accepted unreservedly. On the contrary, since the cost of target hardening eventually falls upon the owner, as a required strategy it can be castigated as "punishing the victim". Here, however, only the technical aspects of security are addressed.

3.5.2 Standards

A British standard, BS AU 209, describes a range of vehicle security precautions. These include:

- vehicle perimeter security (i.e., door, boot and bonnet locks),
- alarms on disturbance or breach of the perimeter,
- immobilisation (i.e., steering and ignition locks), and
- aid in the recovery of stolen vehicles (i.e., vehicle identification and vehicle tracking).

A recent Australian standard, 3749 Part 2, covers the performance and installation of alarms/immobilisers.

3.5.3 Perimeter security

Better locks may improve perimeter security, but any normal window glass may be broken and, therefore, although contactless smart cards might enable more convenient access through the vehicle perimeter than keys, they do not greatly improve resistance to a crude attack, followed by pilfering.

3.5.4 Alarms and immobilisers

Authorities differ about the usefulness of alarms which, in the literature, are often grouped with immobilisers as a single device. Generally, immobilisers merely require the user to present the correct token. Bovelander has drawn attention to Kerckhoff's principle, that security should rely only on the key (not the algorithm) and to the shortcomings of "security by obscurity" as it is sometimes called (Bovelander & Van Renesse, 1995). Unfortunately, most immobiliser vendors do not accept the Kerckhoff principle and are loath to disclose how their devices work. Naturally, their attitude gives rise to misgivings about immobiliser effectiveness against attack by professional thieves.

The British Insurance Industry Vehicle Security Scheme (BIIVSS), out of a total of 964 points allotted for various security features that could be fitted to a vehicle, awards 650 for a properly installed, approved alarm/immobiliser system (Ashley, 1993). At about the same time another British organisation, Partners Against Car Theft (PACT), carried out tests that purported to prove that alarms were ineffective

(Adams, 1993). Livermore, commenting on immobilisers, says defeat by thieves with expert knowledge is certain for "after market" devices, because these electronic immobilisers can all be de-installed (Livermore, 1993). He does not elaborate on this rather surprising statement and most engineers would probably contend that there are many engineering processes that are reversible only with great difficulty.

Apparently the Western Australian Government concurs with BIIVSS and PACT, because, in 1996, it agreed to pay an A$30 subsidy to support the installation of an immobiliser, whilst alarms did not attract the subsidy ("Coalition's", 1996). Since the cost of an alarm/immobiliser that met the Australian Standard 3793 lay between A$300 and A$600 and an immobiliser alone between A$130 and A$200, the subsidy seemed unlikely to alter significantly the public perception of the cost-effectiveness of the devices. By the end of 1997 the WA Government had actually spent only a twelfth of the budget for the subsidy and, under the WA Road traffic Act Section 24(2), has now made fitting an immobiliser compulsory before a vehicle can be licensed or transferred.

In 1996, in WA, about 20% of the State's one million light vehicles were fitted with some alarm or immobiliser ("Car theft action", 1997), and in SA, in 1995, only 13% of stolen vehicles had an anti-theft device activated (Motor vehicle theft in SA, 1995). Perhaps therefore, assuming the proportion of vehicles fitted with anti-theft devices in SA to have been similar to that in WA, the devices do give some protection, since otherwise one might expect vehicles that were stolen to have devices fitted in the same proportion as those that were not (i.e., 20% not 13%).

According to police statistics, in 1999, car theft in WA fell by 19.6%; but the RAC points out that if vehicles subjected to malicious damage or theft of parts are included, the fall is much smaller, and suggests that the reduction could, at least partly, be due to overall improvements to car security systems by vehicle manufacturers ("Fewer", 2000). Anti-theft devices tend to be installed on more modern and expensive cars and, since 1992, all Australian produced cars have had immobilisers factory fitted — but neither expensive, nor recently Australian produced, cars are prominent in the range of cars most commonly stolen – see Appendix 3. All commonly marketed immobiliser systems provide the driver with a token (e.g., a tag or transponder) that de-activates the immobiliser and these tag activated systems have the disadvantage that the tag can be stolen or the driver can fail to activate the system when leaving the vehicle. A smart card could form part of an immobiliser system for a vehicle and, by requiring submission of an encrypted code, could make an electronic attack more difficult. In that case, the driver not only has to have something (i.e., the card) but must also know something (i.e., the code). Furthermore, the card could be programmed to immobilise the vehicle after a suitable delay, so that even if the driver left the card in the vehicle, any thief must then still either discover the code or by-pass the immobiliser system. However, as already pointed out, even a smart card system could do little to thwart the crude type of attack in which the perimeter is forced and the contents looted.

3.5.5 Multi-point immobilisation

In immobiliser design, the more points at which an immobiliser acts the more effective a deterrent it will be, since the thief is put to more trouble in by-passing a multi-point system ("Multi-point immobilisers", 1995). A smart card might provide a code that could be made essential for the operation of any designated electric device, including locks that were electrically unlatched. The number of codes or "differs", to use the language of the British standard, could be quite large. The operation of the fuel and ignition systems might be made to depend on a signal provided by the smart card and, also, without that signal, the "look-up map" in the microcontroller of the engine control unit made unavailable. Inevitably, multi-point protection adds to the cost.

3.5.6 Aids to recovery

Aside from either overt or hidden identification marks, aids to recovery consist of tracking schemes, of which there are several options.

- Land-based schemes that rely on a beacon in the vehicle being located by resection from receiving stations. An example is the QuikTrak scheme in Sydney described by Adams (Adams, 1996).
- Global Positioning Systems (GPS). These use satellite signals, require line of sight, and are used by major fleet owners to track their shipments.

- Some types of cellphone network could be used. For example, the Federal Communications Commission, in 1996, mandated that within five years the technology must be in place to fix the location of callers to within 400 feet.
- If road pricing and congestion control were introduced, the accompanying toll stations could track vehicles.

None of these schemes require the use of smart cards, but tracing a vehicle by means of the cellphone network might be facilitated by their use. The possibility may become the subject of another study and is not discussed further here.

3.6 Improved Convenience

In introducing this chapter mention was made of the additional driver convenience that might be achieved as a by-product of a system to improve vehicle management. Although this benefit is unlikely to be significant for most drivers, for luxury vehicles with power-operated seat and mirror adjustment, a smart card could store the cardholders' preferences and automatically adjust these ancillaries when the smart card was inserted. Similarly, cruise control, radio, CD/ROM and tape players could be set to the holder's preference. In a more futuristic scenario, relating for example to a "drive by wire" vehicle, the card might even contain settings for steering ratio, suspension rigidity, a GPS display or "clear distance ahead" warning (Lammers, 1999).

3.7 Conclusions

A smart card system could probably provide a useful "in-vehicle" alternative to today's manual, on-board automatic logging, or external automatic methods of collecting vehicle management data. System advantages might include generally improved convenience for authorities, fleet managers and, perhaps also, fleet drivers; but owner-drivers might be unenthusiastic. A smart card system might also bring marginal improvements in the accuracy and comprehensiveness of the data being recorded, and the card itself might provide a useful component in security, since it could be the critical part of a locking system, an immobiliser, and at least one tracking system. The tracking aspect might be more attractive to owner-drivers than the preceding ones, but security must be balanced against its cost: a consideration deferred until chapter six. Possibly the greatest improvement would occur if all these measures could be integrated into a single system. Unfortunately, a number of difficulties impede the development of any (especially, integrated) system and these are discussed in the remaining chapters.

4 PROBLEMS AND DIFFICULTIES

4.1 Introduction

Chapter one presents the assumption, amongst others, that smart cards will be used in vehicle management only if their use for other purposes becomes widespread. Chapter two claims that the technology to support smart card based vehicle management either exists or could be readily developed, and chapter three discusses how it might be applied, but concludes with a hint concerning obstacles to implementation. In this chapter, those obstacles that do not relate directly to commercial competition are described, beginning with the need to standardise, reduce costs, and improve smart card capacity and performance to a level that would support a multi-application card. At this point, it should be noted that a multi-application capacity requirement is more demanding than mere vehicle management. Other problems involving security and biometrics are then considered, and, finally, political and individual concerns are addressed.

4.2 Multiple application smart cards

A multi-application capability, precisely defined, is the capability to take a smart card housing one or more different applications, add another application without reference to the applications already on the card, and do this without disturbing the others or taking any special action with the application being loaded. Above, the assumption has already been made that the development of multi-application cards is an essential prerequisite to their use in vehicles. Happily, consumers may also want such a development, as evidenced by the Smart Card Forum reporting a consensus amongst its members to that effect. The Forum quoted research that purported to prove that 50% of members thought the multi-application card would be either excellent or a good idea. Only 15% thought it was a poor idea (Barr, Allen & Burke, 1997, p. 64). The finding is suspect, although plausible, not only because market research is sometimes faulty, but also because the Forum was established in 1993 by Citicorp, Bellcore, and the US Treasury Financial Management Services Division, to accelerate the widespread acceptance of smart cards that support multiple applications. If the development of a multi-application card is essential before smart cards are used in vehicle management, the formidable preconditions for any such development must first be met. A list of essential criteria for multi-application success could include:

- market acceptance of at least de facto standards,
- a potential for long term economies of scale,
- a common technology that is fraud resistant,
- a satisfactory business case for each player,
- the involvement of a high volume but low value application such as transportation or payphones,
- a critical mass of cards in use,
- a ubiquitous infrastructure to accept cards (developed through alliances), and
- brand identification and holder trust in the brand (Allen & Kutler, 1997, p. 15).

As will be seen, these preconditions are, to some extent, aligned with the problems and attitudes that are discussed in this and the next chapter.

4.3 Standardisation

4.3.1 Objectives and obstacles

The smart card industry recognised at an early stage that standardisation would play a major role in the development and acceptability of smart cards (Bannerjee, 1997). Standards are being set which are:

- specific to smart cards, and may be thought of as dealing with either external physical characteristics, or the internal workings of the integrated circuit (e.g., communications and operating systems) or,
- specific to applications rather than the technology, such as those relating to identification and financial transactions (e.g., payments or the electronic purse).

Standards may be the key to ensuring that smart cards and their infrastructures are interoperable, but progress is impeded because the requirement is continually changing as the technology develops and further applications are found. Where standardisation is achieved, confidence in smart card solutions and their attractiveness in meeting business requirements will increase. According to the NZ Future's Trust, quoting the Central Computer & Telecommunications Agency,

> "Smart card manufacturers and scheme operators have a strong desire to develop international standards in order to achieve high levels of interoperability" ("CCTA Report", 1995).

The statement may be true, but the manufacturers and operators also try to ensure that any accepted standard is as close to their own technology as possible, since in this way the effort needed to achieve compatibility is minimised. If this second motivation predominates the result might be a power struggle and delay. Ideally, it should be possible to use any smart card, in any reader, anywhere in the world, but this ideal is a long way from realisation and, indeed, might be realised only with overwhelming inter-industry and international cooperation. The inevitable reduction in variety will be painful for those who have developed unique products, and most standardisation work-groups are about sharing the pain. A further consideration is that, in the process of achieving interoperability, standards must not inhibit technological advances. If the efforts of the official organisations do not produce a standard, eventually, judging by history, a so-called industry standard will become established, which all commercial participants will have to support if they are to operate successfully in the marketplace. An industry standard is, in fact, merely a specification that is being proposed as a standard by some powerful sponsor or consortium of firms.

4.3.2 ISO standards

ISO standards appear to be the most important and relevant agreements, within the framework of which most other standards have been developed. Although already outlined in section 2.3, the essentials are repeated here to provide a basis for the description of other efforts to achieve a degree of compatibility. Standard ISO 7810 covers the dimensions and physical characteristics of smart cards. Communications with contact cards are covered by standard ISO 7816, which has six parts, of which parts one to three define communications with the cards, and four to six deal with matters relating to the card operating system, such as data elements and file structures. Parts seven and eight are still in draft, but will extend parts four to six. Parts nine and ten are in an earlier draft stage, and will define further inter-industry commands and protocols for synchronous communications, respectively. Contactless cards are covered by two standards, ISO 10536 for close coupling, and a planned standard ISO 14443 for remote coupling (Fancher, C. , 1997). A proposed standard for vicinity cards, ISO 15693, is not yet even in draft. There are a number of other ISO standards, but they have little relevance to the use of cards in vehicle management. It should be noted that Japan has its own independent standards organisations (e.g., JEIDA) that are also active.

4.3.4 Standard card operating system

If the card itself could be standardised, the next most important aspect might be the card operating system. To date, smart card issuers have written what are essentially proprietary applications that are integrated with the card operating system and are not interoperable or portable. For a combination of technology, cost and security reasons mentioned in sections 2.3 and 2.7.12, few chipmakers offer a smart card chip that does not have at least part of an operating system hardwired as part of the integrated circuit. Even fewer firms offer smart card operating systems that are not designed for a specific chip (Guthery, 2000). Consequently, there are at least a dozen different smart card operating systems offered by various hardware and software vendors. It would seem that if multi-applications are to be successful, there is a need for standard open platforms on which to develop smart card applications quickly; including those that are supplementary or "after issuance". Application issuers must be convinced that another (genuine or fraudulent) application on the same card cannot interfere with, or otherwise affect, their own (see section 4.2). Alternative proposals to achieve this situation are offered by several industry groupings.

4.3.5 MULTOS

Mondex and MasterCard, with cardmakers Gemplus and Dai Nippon and chipmakers Motorola, Hitachi and Siemens, (but, significantly, excluding Visa) promote an "industry standard" operating system, MULTOS, that seeks to ensure that multiple applications may reside on a single smart card without interfering with each other. MULTOS is claimed to be the first open, high-security, multi-application operating system for smart cards, enabling a number of different applications to be held securely on the card at the same time. Its promoters say it may open up the smart card market, creating new avenues of convenience for users while delivering savings and opportunities for the industry (MULTOS, 1997).

4.3.6 Windows for Smart cards

Recently, at the Cartes '99 Paris convention, Microsoft arrived on the scene as a powerful latecomer with Windows for Smart cards. Microsoft has promoted its operating system not only for network security, but also for health, payment, loyalty and, more recently, subscriber identity module (SIM) cards for the GSM cellular phone market. At the convention, the accompanying toolkit to enable developers to write SIM card applications using Visual Basic was expected to become available early in the year 2000 ("Microsoft releases", 1999), but at the time of writing (June, 2000), there had still been no report of its release.

4.3.7 Java API

As a consequence of the lack of a standard card operating system, only with difficulty can applications operate with cards from different vendors. One solution is to install on the card a program called an Application Programming Interface (API) that will translate application commands into a form readable by a range of cards and their operating systems. JavaSoft, a business unit of Sun Microsystems Inc., with some support from other industry leaders, (including Visa) has claimed that the Java Card API 2.0 will solve this problem ("Sun Microsystems", 1996). Sun Microsystems claims that:

- the Java Card API is a specialised Java application interface, optimised to provide critical Java functionality to smart card developers, and

- is the first industry standard language and open API for smart cards that allows applications to run on all standard ISO 7816-4-compliant smart cards.

Java's scalability and platform-independence are said to provide the ideal environment for creating smart card applications, a standardised process for adding new features and changing old ones, and clearly established commercial terms describing the rights and responsibilities of participants. Unfortunately, it seems that, at least until recently, each card manufacturer defined its own Java byte code set, and so it is probably not possible to take an applet of the card of one manufacturer and run it on the card of another (Guthery, 2000). Gemplus and Schlumberger, who together make about 70% of all smart cards, support the Java Card API ("Smarter Java", 1997). But, see earlier paragraph, Gemplus also supports MULTOS! However, the financial institutions, which are likely to be the most powerful issuers, will probably determine the outcome. Siemens, the third largest card maker, also appears to be keeping all options open because, in July 1997, it licensed Java technology from Sun Microsystems ("Sun and Siemens", 1997). An open system, or operating environment, like Java Card, encourages widespread support, because there are published specifications about how the environment works. The Java API may be thought of as an adaptor between, on the one hand, any of a range of operating systems or chip instruction sets, and, on the other, selected Java programs and applets: however, it is probably a memory and power hungry solution as illustrated more fully in section 7.2.1 and Figure 16.

4.3.8 Backend software

Another, somewhat different, potential solution to the problem of multiple non-standard operating systems relies on a suite of software that resides partly on the cards and partly on the terminals that read and, if necessary, write to the cards. One proposal, known as the OpenCard Framework, comprises three software layers, two of which (CardService and Application Management) reside on the card and effectively adapt the card's operating system to match the other layer (CardTerminal) that resides on the reader. It is Java based, but in this way, at some cost in card processing resources, many smart card types may be enabled to work with almost any reader. A consortium that includes IBM, Visa and American Express (but excludes MasterCard, Hitachi and Mondex) promotes the framework (OpenCard Framework, Oct, 1998). A second related concept, is Visa's Open Platform, which is being promoted by GlobalPlatform, an organisation whose primary objective is the development and publication of standards and specifications that might be used by companies implementing multiple application smart card programs. The Open Platform is said to enable the fast and easy development of globally interoperable smart card systems, and is comprised of three integrated elements: the card specifications, the terminal specifications, and the workbench tools. The concept seems to be similar to that of the OpenCard Framework, but the organisation claims to be different from the Framework's consortium in that it has a "cross industry" membership and, indeed, it includes several telecommunication companies, known as telcos, but no major financial institution ("Open Platform", 2000).

4.3.9 Electronic payment standards

Even if a standard operating system, or an acceptable alternative, emerges, there would still be a need for standardisation within applications. One of the most important application areas relates to electronic payments. Whilst awaiting the promulgation of an official payment standard, which, hopefully, will be incorporated into the ISO framework, a specification has been developed by Europay, Mastercard and Visa (EMV), that covers the interaction between smart cards and readers for all payment system applications (debit, credit and offline) (Rankl & Effing, 1997). The specification was intended to create a common technical basis to compete with Mondex specifications: at the time MasterCard had not purchased control of Mondex. The EMV specification is a substantial document that aims to ensure that any payment system smart card may be read by any reader if both conform to the standard, but, according to some manufacturers, it is actually not quite specific enough to achieve this aim. The first version was based on cards with symmetric encryption and the matter of key transportation was unresolved ("What contains", 1995). The EMV standard was declared by its sponsors to be "functional" in 1996, but many large, particularly French, applications do not conform to it. The Estonian Institute of Cybernetics has provided a summary of the contents, grouped into three parts:

"Part I: Electromechanical Characteristics; Logical, Interface, and Transmission Protocols

This part of the specification concentrates on physical and logical elements of the interaction between smart cards and electronic terminals used for payment transactions....

Part II: Data Elements and Commands

This part defines data elements and files, the commands required to execute financial transactions and terminal requirements. When data elements are exchanged between cards and terminals, they become data objects. These objects can be simple or complex depending on how they have been processed. All data objects reside in data files. Data files in a card, when viewed from the terminal, appear in a tree structure whose main branches are application definition files that are application-specific. This structure allows diverse applications to be maintained separately within a single card....

Part III: Transaction Processing

This part defines the content and flow of payment transactions for both cards and terminals, establishing common core functions for international interchange transactions. However, card issuers may also create functions that are unique to specific applications and payment systems...." ("Technology/smartcards", 2000).

4.3.10 Common electronic purse specification

A specification being developed by the Comité Européen de Normalisation (CEN), prEN 1546, covers the electronic purse. Apparently in an attempt to pre-empt other efforts to develop an industry standard for the purse, in March 1999, a consortium "released" the common electronic purse specification (CEPS). The specification, reportedly, is based on the former CLIP purse system discussed briefly in the next chapter. The consortium consisted of CEPS Co of Spain, Kartensysteme of Germany, Europay and Visa. Mastercard, which owns the Mondex system, is not a member (CEPS, 1999).

4.3.11 PC/SC specification

Another effort to produce an application specific specification, by a consortium of leading companies from the PC and smart card industries, seeks to promote the acceptance of smart cards in the PC/Internet environment. The intention is to develop a set of open standards enabling PCs to work with such smart card applications as network access; especially in electronic commerce. In particular, the Workgroup members identified the need to standardise interfaces to readers, and considered the specification of common PC programming interfaces and control mechanisms as critical areas to be investigated ("PC/SC Workgroup overview", 1996, September 12). If the effort is successful the conforming smart card readers will become, in effect, standard PC peripherals. Microsoft's "Windows for Cards" appears to be the first operating system to support the "standard". A second version of the specification is being drafted ("PC/SC Workgroup specifications update", 2000).

4.3.12 MIFARE

Yet another application area that would benefit from standardisation is transportation ticketing. Since the standard ISO 14443 for contactless card communications is still not finalised, it seems likely that the European standard, CEN1545, for data elements in contactless cards, or de facto standards such as the Philips designed MIFARE system, will dominate these applications for some time. However, both Motorola (now Atmel) and SGSThomson (now STMicroelectronics) have announced that they intend to develop cards based on ISO 14443. The two makers claim to believe the planned ISO standard provides better security and wider interoperability than MIFARE (Costlow, 2000).

4.3.13 Other standards organisations

A number of other organisations are attempting to establish standards for smart cards. Probably the most successful of these is the European Telecommunications Institute (ETSI) which has achieved worldwide acceptance for the Global System for Mobile Communications (GSM) card used in one mobile telephone system (Guthery, 2000). Another example is the National Committee for Information Technology Standards (NCITS), formerly the American National Standards Institute (ANSI), that has produced a standard for a driver's licence on an electronic card

(Electronic, 2000). There are several commercially sponsored groupings purporting to further standardisation but, alas, they are probably driven more by marketing agendas than any technical necessity.

4.3.14 Certification authority model

Standardisation of smart cards, their operating systems and key applications may not be all that is required for interoperability. Robin Townend, of Intellect Australia Pty Ltd, a Perth manufacturer of smart card readers with international standing, says there are two issues blocking the faster rollout of smart cards and that a common and open operating system is only the first. The second is the need for banks to work out a certification authority model ("Curly questions", 1997). A certification authority is a trusted third party that issues and manages credentials in the form of certificates for individuals or entities. Commonly, the authority checks with a separate investigating body to verify information provided by the party requesting the certificate. All over the world, organisations are setting themselves up as certifying authorities. Within Australia, SecureNet, a Melbourne company, is offering to address this second issue with three forms of digital certificate (personal, corporate and server).

Economic considerations

4.4.1 Cost estimation

All estimates of the future cost of smart cards are based on two assumptions:

- the cost of electronic circuitry will continue to fall, and
- a mass market will emerge.

Before either a multi-application card or a "killer" application appears, costs may need to be reduced. Put another way, if a mass market is to be developed, the cost of smart cards must be kept low. With an estimate in 1992 that, by 1995, the annual market would be one billion cards, it was expected that, by then, the cost of a smart card would be US$3.00 (Baker, 1992). Neither the volume, nor the cost, was achieved (Amdur, 1997).

4.4.2 Components of system costs

The cost of a smart card system is more than the cost of the cards themselves. Other costs are:

- hardware peripherals, such as terminals or readers,
- software, for both smart cards and their infrastructure,
- network costs, and
- enrolment of users (Svigals, 1994).

Svigals does not mention the development costs of applications, which would need to be taken into consideration. There might be comparative gains for smart cards amongst these other costs. For example, costs in validating current magstripe cards at EFTPOS terminals might be reduced if smart cards were used, but probably would not vanish. Against the costs of smart cards must be offset benefits, such as the potential reduction in fraud, and the greater durability of smart cards.

4.4.3 Card costs

A comparison of the cost of magstripe and smart cards follows.

Table 2: Magstripe and smart cards compared

Parameter	Magstripe	Smart card
Life (years)	2	10
Cost (US$)	0.10 to 0.50	1.00 to 20.00

The life of a smart card is estimated to be 10 years, versus two years for a magstripe card, but smart card cost estimates vary greatly. (It may be worth noting that the primitive smart cards used in the simulation to be described in chapter six, cost A$20 each.). Duffy estimates that a complete smart card might cost US$1.00 to US$20, whereas a magstripe card might cost from US$0.10 to US$0.50 (Duffy, 1996). His estimate makes no mention of the cost of embedding the chip in the card. Cordonnier, in 1995, gave the average price of a card as US$4.00 (Cordonnier, 1995). In 1997 he estimated the average cost of a smart card, including its share of the infrastructure overhead, as US$20, and the cost of a contact smart card as from US$2.00 to US$10 (Cordonnier, 1997). In the earlier estimate he may have been including memory cards and in the later one contactless types, but, even so, does not appear to be able to report that costs are falling. The Gartner Group provide different estimates again.

Table 3: Magstripe smart cards and optical cards compared.

Card type	**Maximum Data Capacity**	**Processing Power**	**Cost of Card**	**Cost of Reader and Connection**
Magnetic Stripe Cards	40 bytes	none	$0.10 - $0.75	$750
Integrated Circuit Memory Cards	1 Kbytes	none	$1.00 - $2.50	$500
IC Processor Cards	8Kbytes	8/16-bit CPU	$7.00 - $15	$500
Optical Memory Cards	4.9 Mbytes	none	$7.00 - $12	$3,500 - $4000

Source: Gartner Group (Stand: June 98). All costs are in US$.

4.4.4 Components of card costs

Components of the cost of the card itself include the plastic rectangle, estimated at US$0.45 to US$0.55. In 1996, assuming mass production, the chip was estimated to cost from US$1.00 to US$2.50, but this cost was expected to fall to US$0.75 - US$1.50 by 1997 (Duffy, 1996).

In tabular form the estimated cost of contact smart cards could be as follows.

Table 4: Smart card costs

Component	**Cost (US$)**
Microchip	$1.00 to $2.50
Plastic card	$0.45 to $0.55
Embedding	N/A

Although the cost of embedding the chip in the card must be recognised there is no published information available as to what the cost might be.

4.4.5 Other costs

Even a basic reader is estimated to cost more than US$100, whilst retrofitting a magstripe reader, for example an ATM, to read smart cards might cost from US$2,000 to US$3,000 (Duffy, 1996; Fancher, 1997). Consideration of what a smart card supported vehicle management system might cost, and what owners might be prepared to pay for it has been left until chapter six.

4.4.6 Cost trend

It appears that the fall in costs expected by Baker did not happen and, even now, there is no evidence of any such trend. Perhaps, instead, gains from more efficient production are being absorbed in developing improved cards.

4.4 Card capacity and performance

4.5.1 Required capacity

Chapter two gave an indication of the potential for increased chip power, but the question now to be addressed is whether or not any increase might be enough to provide a multi-application capability. Assuming costs can be kept at an acceptable level, if smart cards are to be attractive to all parties (issuers, financial institutions, merchants and the public) and are to support multiple applications, then they will need to provide on-card, asymmetric, encryption facilities, and, eventually, biometric identification. A multi-application capability is expensive in computing resources, and encryption even more so ("CASCADE FIRST", 1994). The definition of multi-application capability in section 4.2 implies that the applications may belong to different entities and be loaded at different locations, that inter-operability has been achieved, and that applications must be isolated from each other. This ideal open system does not appear to be imminent, but, when and if it arrives, it will almost certainly make further claims on the limited chip resources. Finally, biometric identification, for true security, should match supplied and recorded features on the card itself, rather than merely supplying a template for comparison elsewhere. Smart card chips will need to improve in both speed and memory if they are to meet these requirements. With the exception of the CASCADE chip, until recently, the chips being promoted or used, for reasons explained earlier, seem intended for financial applications and have little spare capacity for anything else ("Motorola", 1997).

4.5.2 Extensibility and personalisation

Two further terms need definition. In the smart card context, extensibility is the ability to add further applications to an existing smart card. Hitherto, in general, extensibility has been limited because an application written for one smart card type could not be installed on another; a problem already discussed under standardisation.

Personalization is the process of taking a "generic" smart card and customising it with data that are specific to a single-application or multi-application card and the individual cardholder. While identification data might be inscribed on the plastic, to personalise the cards the programmer will need to embed personal statistics in the chip and customise applications stored on the chip. The process, an essential service to implement any smart card applications system, is conceptually identical to the personalisation of vehicles and cellphones, being merely different in implementation. Personal identification is essential to provide secure access for smart card holders to premises or company networks, and Internet or other electronic commerce applications. Mere possession of the card should not be sufficient. Personalisation also enables issuers to build brand recognition and customer loyalty by enhancing frequent shopper and similar loyalty programs ("Standard Register partners", 1997). Ease of both extensibility and personalisation is important for issuers and those employing smart cards as part of an application. The facility might not be relevant to vehicle management, but it must be borne in mind that for the smart card to be accepted for vehicles, it will need to have other uses.

4.6 Security

4.6.1 Aspects of security

Although smart card technology is making steady advances, most mass markets have not yet used it to anywhere near its potential. One reason may be that for many applications such as electronic purses, bankcards, pay-TV cards and phonecards, it has proved almost impossible to achieve the high level of security demanded at a low enough cost. If a smart card is to be used to improve the security of facilities or systems, then the card itself must be secure, and unauthorised persons should not be able to counterfeit it, read it, manipulate its contents, or use it. Security may be considered at the chip level, the card level, the application level, or the system level. Breaches might be systemic or individual. E. T. Patrikis, First Vice President of the Federal Reserve Bank of New York defines a systemic risk as "... the risk of an event which could bring markets or clearing and settlement systems to a halt, or cause the failure of additional market participants." Elsewhere, more succinctly, he refers to systemic breaches as "show-stoppers" (Patrikis, 1996).

4.6.2 Systemic

At the individual level, a fraudster might possibly discover the PIN (or biometric template) of an individual and abscond with money or gain access to information. The individual concerned could be severely inconvenienced, if not ruined, but for the issuer the loss would probably be supportable. However, in some future, smart card supported, global financial system, if criminals found a way to counterfeit cards, the world's financial system might be destroyed in an attack similar to that attempted by Germany against Britain during World War II (Bank of England, 1997). In this attempt, a large number of five pound notes were allegedly scattered over Britain by airdrops. Although subsequent reports claim the notes were used to finance Germany's spy system and found there way to England indirectly (Hottl, 1955), whatever the distribution route, the notes were indistinguishable from the genuine item and, as a result, no financial institution or merchant would accept the denomination until a new issue was made with a distinctive gold wire through it. Many people holding perfectly genuine notes suffered loss. An often-perceived advantage of cash money is anonymity, but the flip side of anonymity is risk. If a hacker was able to counterfeit DigiCash or Mondex cards, the entire currency might become worthless ("Timorous trade", 1997). A somewhat different systemic breach might occur if, through a failure of non-repudiation, an individual could prove that a withdrawal from the deposited money had been taken by fraud. No doubt the deposit taker (presumably, the card issuer) would be obliged to make good the individual's loss and, thereafter, dishonest people could claim that withdrawals they had actually made were the work of fraudsters: to the great embarrassment, if not loss, of the deposit taker.

4.6.3 Chip level

Chip security begins with the design of the chip, which is arranged, not only for efficiency, but also for the protection of the stored data: therefore, the design team usually includes the card manufacturer's representatives. Chips must be manufactured in as secure an environment as are, for example, banknotes; so, all chips, whether acceptable or faulty, must be accounted for (Baker, T., 1992). Chips normally may be operated in one of three modes; test, development or user.

- The chip manufacturer must be able to test the chips.

- The card manufacturer must be able to develop the chip, usually by adding programs to the non-volatile, rewritable memory and ensuring that these programs cannot be tampered with.
- The application developer must be able to add still more programs and, similarly, prevent further tampering.

Before the card reaches the user, the test and development modes should have been irreversibly disabled. Various techniques are used for this purpose, amongst which are:

- providing a power spike to the chip that causes essential, polycrystalline silicon, fuses to 'blow'; and
- precision sawing to remove part of the circuitry (Myers, 1996; Paterson, 1991).

Delivery must be handled in a secure manner similar to that used for banknotes or bullion (Paterson, M., 1991), and any attempt to tamper with the chip should cause it to self-destruct (Myers, 1996; Paterson, 1991).

Finally, until recently, a single chip was used because, among other problems, multiple chips may have connections that are vulnerable to attack: a consideration that limited the size and, hence, the power of the chip circuitry. Since, as already mentioned in section 2.7, a dual-chip card is being trialed in China, it might seem that this restriction on multiple chips had now been relaxed, but that is not the case as the two chips on the card are not connected.

4.6.4 Chip cracking

Despite all these precautions, chips probably may be reverse engineered or "cracked". At least four groups claim to have proved that it can be done.

The first was Bellcore Labs. Julie Krueger, acting executive director of the Smart Card Forum, and Rebekah Schloss, senior product manager, InterBold, and member of the Forum's board, have commented on the Bellcore research.

> "In September 1995, Bellcore announced a theoretical technique to crack a smart card or other RSA cryptographic processor by inducing faults through mechanical means, and monitoring the resulting changes in the output ciphertext. The press coverage that followed cited a number of authorities whose conclusions, in general, are that the technique, while it is only theoretical, is important for the industry to be aware of, and cracking one smart card through a rather elaborate scenario does not compromise the security infrastructure." (Krueger & Schloss, 1996, p. 1).

The second group comprised a team of researchers from Cambridge University, which, under the leadership of Professor Ross Anderson, categorised a variety of types of attack on the security of smart cards. The team had in mind the increasing number of systems, from pay-TV to electronic purses, that rely on the tamper resistance of smart cards and other security processors, and, hence, the team described a number of attacks on such systems - some old, some new and some that are simply little known outside the chip testing community. The researchers concluded that trusting tamper resistance is problematic: smart card security is routinely breached, and even a device that was described by a government signals agency as 'the most secure processor generally available' turned out to be vulnerable. Designers of secure systems were advised to consider the consequences with care (Anderson & Kuhn, 1996). However, an unsigned web page by Semiconductor Insights Ltd sets out to rebut the Cambridge team's claims. Its rebuttal depended mainly on the contention that the microchips attacked by the Cambridge team were chips with parallel ports, unlike those used in smart cards which have only a serial port and a reset ("TAMPER RESISTANCE", 1996).

The third group was from an Israeli University. According to a report by Markoff in the New York Times, two Israeli scientists, Adi Shamir, a professor at the applied mathematics department at the Weizmann Institute, and Eli Biham, a member of the faculty of the computer science department at the Technion, reported that, in addition to the so-called public key coding systems that were found vulnerable by the Bellcore team, private key data coding systems, such as the American Data Encryption Standard, or DES, might be successfully attacked if a computer processor can be made to produce an error (Markoff, J., 1996).

The fourth group, Cryptography Research, a private consulting company in San Franscisco, was reported in the New York Times to have used a technique that relies on the fact that semiconductor chips must use electrons to do calculations. The Company showed, for instance, that the key from an RSA system might be extracted by watching an oscilloscope graphing the power consumption of a card (Wayner, 1998). Some counter measures were also mentioned.

4.6.5 Counterfeiting

Counterfeiting, a different form of attack, has evoked conflicting comments. Stephan Seidman, editor of the Smart Card Monthly, wrote in 1994 that, in twenty years, not one counterfeit smart card had been reported anywhere in the world (Seidman, 1994). Strangely, Svigals, at about the same time, quoted a Wall Street Journal report of a 1992 cellular phone system probable revenue loss of US$400m, due to chip based fraud. The attackers got good identification numbers from cellular transmissions, and replaced the ID chips in the cellular phones with general-purpose chips programmed to emit the pirated identification numbers. One massive attack used modified cellular phones for a week and then discarded them (Svigals, 1994, p. 111). More recently, the Smart card Developer's Association (SDA) and two UC Berkeley researchers announced that the GSM SIM card could be cloned. Although this was a research exercise and not an actual theft, the potential for peculation was demonstrated. In addition, the association drew attention to other weaknesses which, it alleged, were partly due to government agencies requiring that confidentiality be weakened (SDA clones digital GSM cellphones, 1998). Therefore, it seems likely that, as with telephone SIM cards, other smart cards could be counterfeited, stolen, or misused. It is possible that the fear of a similar systemic breach has played a part in the reluctance of financial institutions to implement the electronic purse, or wholeheartedly to support electronic transactions.

4.6.6 Card

Apart from the chip, it is possible to make the card itself difficult to counterfeit. The materials used are not easy to work with, and features could be included analogous to the watermark, or hologram, of a banknote. Even laser engraving, which burns a subsurface layer of the plastic, is a fairly secure print, and can be removed only with great difficulty. It should be born in mind, however, that a bogus card will probably not be used in the presence of the person being deceived. The bogus version often does not need to look like a genuine item, only to behave like one.

4.6.7 Application

At the application level, the card may provide a cryptographic facility that helps to protect information stored in it, and the facility could be enhanced by an asymmetric "challenge and response" protocol, to render the card virtually proof against spoofing and masquerading. Unfortunately, protocol protection uses a lot of the "on-card" computing resources (Leach, 1995). Although the card's processor security is capable of being controlled by the card issuer (through the card personalisation process), the control comes with an additional need for a secure key management system to be designed and implemented. In most 'smart card based' applicat'ons, the business users have to take the word of the smart card vendors that security has been properly implemented, and trust that they will not abuse their privileges. Another problem relates to card testing. Because of the security protection that is built around the chip, most of the security features of the smart card logic cannot be tested without blocking the card or destroying it. Any tests, even if identified, may have been performed only on a small production sample (Kang, 1996).

4.6.8 Security Certification

The creators of smart card products may obtain security endorsement through the Information Technology Security Evaluation (ITSEC) or Common Criteria schemes. The procedure involves:

- a claim by the product sponsor as to the degree of security offered by the product, and
- a rating under the scheme that represents the extent to which the product achieves the sponsor's claim.

This kind of certification is not totally satisfactory because not all users may be aware that a high rating might be merely a consequence of a modest claim. Nevertheless it is not easy to see how a more stringent system could be devised (Reid & Looi, 2000).

Biometrics

4.7.1 Performance

Biometric identification has been suggested as a partial solution to the security problems impeding the widespread use of smart cards, but requires sophisticated expensive hardware; and, although smaller biometric identification devices are in sight, size is still a problem for mobile applications (Kim, 1995). Furthermore, the use of the image of any human feature depends on computationally intensive image registration techniques (already described in section 2.4) and are currently beyond the capability of any smart card processor. In current systems the smart card is used to store a template of the biometric feature of the card owner, and the creation of a matching template from a supplied feature, followed by any comparison of the two, is undertaken elsewhere, using a more powerful processor; a technique that fails to exclude the possibility that the communication between the card and the computer could be intercepted, and the system breached by manipulating the communication. If the work of comparison is to be done in the card, more powerful card processors will have to be developed, or simplifications found. A major problem is that the banks require a False Rejection Rate (FRR) of less than 1 in 100,000 (Carter, 1995, p. 3). In this connection, MYTEC, a leading designer of biometric identification systems, has published the following statement about the performance of its system:

> "FAR: (type 1 error) False Acceptance Rate is when someone other than a legitimate user is accepted. MYTEC Targets: FAR1/10,000.
>
> FRR: (type 2 error) False Rejection Rate is when the legitimate user is not recognised by the system. MYTEC Targets: FRR1/100,000. These numbers are industry specifications, and as we are currently testing large populations, we are confident that the MYTEC system will exceed these specifications."
>
> ("MYTEC Training", 1996).

It is difficult to share MYTEC's confidence, because no independently tested system has achieved anything approaching that performance, and other vendors' claims are still an order of magnitude from it. National Registry Inc. (NRI) in conjunction with

Unisys claimed, at the American Bankering Assoc. conference in May 1996, to have met the banking requirement, but released no actual figures ("NRI at ABA Solutions", 1997 Feb 10). Financial institutions are believed to argue that false acceptance is a less grievous fault than false rejection, because, for a potential intruder, it makes no difference if the chance of penetration is one in 10000, or only one in 100 (Carter, 1995). In either case the intruder will probably be discouraged and think twice before attempting to intrude; whereas, even occasional false rejection might result in a ruinous loss of custom.

4.7.2 Certainty of uniqueness

False acceptance may be considered from a different angle. Identical twins have identical hands and will experience little trouble in being identified as each other with the hand geometry method, and even between family relations the false acceptance for hand geometry is probably much larger then the false acceptance for randomly chosen people. Fingerprints, on the other hand, are the result of a genetic random process, and fingerprints of identical twins or other family relations are believed to have no correlation (Miller, 1994). Therefore, when choosing between fingerprints and hand geometry, there is a logical bias in favour of fingerprints.

4.7.3 User acceptance

User acceptance might be an issue for smart card system developers attempting to use biometric identification. An ECU study showed that for many people the intrusiveness of the collection method, the length of the enrolment time, the likelihood of system failure, and the speed and throughput rate at the time of use, were all major issues affecting the acceptability of an application. A framework for the treatment of the issues was developed, but its effectiveness has not been tested (O'Loughlin, 1998).

4.7.4 Testing

The testing of biometric identification methods still poses great difficulties and a key issue for the Biometric Consortium's National Test and Evaluation Center (now known as the US National Biometric Test Center) was the development of test and evaluation method(s) for repeatable statistically-significant performance tests. The main question the Test Center sought to answer was as follows: how might testing technicians obtain reliable receiver operating curves (ROC) from a device, and make meaningful comparisons with ROCs of other, possibly non-biometric (e.g., password), devices? The Center listed a number of subordinate questions grouped according to whether the tests use humans, simulations, or recordings/reproductions respectively.

- If a human sample is used, how are the individuals selected and calibrated? Will the same humans be needed for all future tests, or can a sufficiently large sample be used to make this unnecessary?
- If simulations are used, what types of simulations will be used, and how will they be used? If fabricated body parts are used, how shall they be constructed and used?

- If recordings and reproductions are used, how will the sensor and recognition system be separated?

This last question directs attention to a difficulty peculiar to the group. In voice systems the sensor (e.g., a microphone) and the verifier are usually separable, and speech may be recorded and the exact record repeatedly played back into the device. For multidimensional verifiers/identifiers (e.g., image-based systems), there is a difficult problem, because some use adaptive scanning, thus making the sensor and the verifier inseparable and the repeated use of exactly the same image impossible. Different devices might also require different illumination, poses, and resolution, further complicating the recording of a database (Campbell & Alyea, 1995).

4.7.5 Industry testing and certification

Presumably because of slow progress by the Biometric Consortium, a number of USA vendors of biometric ID systems have formed the International Computer Security Association (ICSA), whose main task is to raise the level of public confidence in biometric identification, whilst improving the accuracy and applicability of each product. To accomplish the task, it undertakes the testing and certification of biometric identification products (ICSA, 1997). Another group, the International Biometric Industry Association (IBIA) represents the biometric industry (i.e., scanner) manufacturers. Yet a third group, the Biometrics Authentication Programming Interface (BAPI or BioAPI) seems to represent the computer industry. To date none of these groups appear to have captured the complete confidence of major potential purchasers.

4.8 Political and individual concerns

4.8.1 General

A number of political and individual concerns may be significant in impeding or promoting the widespread use of smart cards, although only indirectly relevant to their possible use in vehicle management.

4.8.2 Tax avoidance.

Governments may be concerned about tax avoidance. There is a perceived risk that an individual with a source of income in a low income tax country could use a smart card in conjunction with a PC/SC application (as described in section 4.3) to live, and spend the income, in a high tax country without paying the higher tax. Although the financial systems and on-card applications necessary for this activity are feasible, no reference has been found suggesting they are available.

4.8.3 Hot money

It is sometimes contended that the widespread, uncontrolled use of electronic purses could make management of national financial systems difficult, and that the unregulated movement of "hot money" might destabilise governments. The term is used here in the sense defined by Walter Wriston:

> "Money that can move. If you get nervous and pull everything out of the market, at the end of the day you'll be holding hot money." (Wriston, 1996).

This is a different concept from "dirty money" (the proceeds of illegal activities), formerly called "hot money". The annual turnover survey results published by the Bank of International Settlements, show that the average daily turnover of global exchange markets in spot, outright forward, and foreign exchange swap contracts, was estimated at US$1.2t in 1995 (Patrikis, 1996). Today, 1999, the daily flows probably exceed US$2t. These money flows take place over dedicated networks, not the Internet, and, as the Asian financial crisis showed, they are capable of destabilising governments; but, smart cards are probably not involved. Relative to the total of "hot money", money transfer by means of electronic purses seems insignificant. Estimates of global monetary flows have been relegated to Appendix 4 but, in section 5.3.7 are briefly related to accrual transactions.

4.8.4 Dirty money

Another concern is that money laundering might be facilitated. In certain circumstances this could be so, since, if there was no limit to the amount that could be loaded onto a smart card, dirty money in an electronic purse would certainly be easier to carry and conceal than the suitcases full of notes that are popularly supposed to be used. However, the law could prohibit "open limit" purses and be enforced in the same way that large cash transactions are today monitored through the banks, so the contention probably carries no great weight.

4.8.5 Consumer choice

Even if the problems discussed in the previous paragraphs could be solved, Governments might still be nervous about the widespread use of smart cards. In addition to public hostility to the perceived invasion of privacy and potential for surveillance, discussed in the next paragraph, consumer advocates contend that there is a chance that individuals may be deprived of choice. Today, despite their legal right to do so, many workers feel too insecure to demand their wages in cash. Instead they accept, in some cases reluctantly, their employer's insistence that wages be paid by bank transfer, and the banks' imposition of fees for the service. Consumer advocates contend that a similar situation could develop with electronic purses. People might be given no choice but to use them, and be forced to accept whatever charges are levied ("Smartcards", 1996).

4.8.6 Consumer protection

Anyone, who is cheated, defrauded, or even suddenly impoverished as a result of a smart card shortcoming, may be expected to call on his/her government for help. If, for example, a purse card issuer failed financially and was no longer be able to redeem the tokens that it had sold, a government could be put under pressure to indemnify the losers. Naturally this possibility makes politicians wary. On the other hand, governments, particularly local governments, will probably be supportive of schemes to use contactless cards as access tokens for public transport, because there is perceived to be a need to improve the image of public transportation, and persuade the public to minimise the use of private cars (Higgs, 1996).

4.9 Privacy and surveillance

4.9.1 Perception of privacy

According to the US Smart Card Forum, in the arenas of consumer acceptance and policy development, no issue is more visible or important than privacy (Allen & Kutler, 1997, p. 248). As a result, smart card business propositions will only be successful if consumers, policy makers, and all other parties, understand the role card technology could play in protecting privacy, whilst efficiently and securely delivering services and benefits. While privacy has many meanings, in the consumer context it is commonly defined as:

- the consumer's interest in knowing
    - how his/her personal information will be used by business or government agencies, and
    - the benefits which will accrue to the consumer from such use, and
- the extent to which the consumer can choose to limit, or prevent, that use (Consumer privacy, 1994; Allen & Kutler, 1997, p. 76).

Invasions of privacy may be grouped into three categories; surveillance, the scanning of databases for information to be used for reasons other than those for which the databases were created, and unjustified identification.

4.9.2 Surveillance

Surveillance, probably the least controversial infringement of privacy, may be defined as the activity whereby logical or physical areas are kept under intermittent or continuous scrutiny, but individuals are identified only if unacceptable behaviour is detected. Examples are the videotaping of football crowds, or the analysis of expenditure patterns for anomalies.

4.9.3 Control of personal data

Clearly, the use of smart cards will raise social issues. A privacy policy could begin with the premise that the cardholder owns the data on the card, and should have defined rights and responsibilities concerning them. For example, the policy could enunciate the holder's

- right to know
  - what data are stored on the card,
  - the uses to which those data are to be put and
  - the benefits accruing to others as well as to him/herself, and
- right to seek remedies if, in the holder's opinion, the data are not accurate.

The policy could also define the limits within which the holder could control the accumulation and use of the data ("Cashless society", 1995). From a different point of view, corporations and others who are contemplating using the features of the smart card to encrypt sensitive information, are concerned that governments might legislate to ensure that the encryption method embodies a facility to enable authorised officials to read the encrypted information (Wriston, 1996). Although there is nothing new in such legislation, it may be regarded as authorising scanning and, hence, an invasion of privacy.

4.9.4 Unjustified identification

It has already been argued, in section 2.4.1, that accountability, for which a possible definition is 'the matching of individuals to their actions', begins with identification. The identification of individuals is important to many government agencies and corporations, because it contributes to efficiency and the control of fraud, and may offer benefits to clients as well. Indeed, a focus of information systems security in recent years has been the intensification of efforts to establish identity. Identification involves conflict between two conditions. On the one hand, flawed identity checking results in duplication, fraud, disruption, costs and risks; and, on the other, rigorous identification is invasive, and its effectiveness may be undermined by unpopularity, falsification and evasion. Biometry, a promising but as yet uncertain identification technique, is, in many senses, merely an extension of natural methods by harnessing technology. Whether the public senses a danger in the establishment of such an extension will depend on its sensitivity to privacy. High-quality identification offers the promise of the avoidance of error and fraud, and privacy advocates often have difficulty expressing their opposition to it; nevertheless, the use of biometrics needs to conform to the standards and expectations of the public. General-purpose schemes may represent a threat to the fabric of contemporary society (Davies, 1994), but even specific-purpose biometric schemes raise issues which need to be addressed. As Clarke puts it,

> "Where transaction trail data are gathered and processed by corporations with an interest in marketing, the activity is viewed by many people as consumer manipulation. Where governments do this, it may represent anything from a balanced and fair mechanism for protecting the public purse, to an oppressive exercise of power by the State over the citizen. ... There are inevitable and necessary compromises that have to be made to privacy interests, in order to achieve a satisfactory mix, and privacy issues accordingly generally involve an exercise of discovering a suitable balance" (Clarke, 1996, p.13 & 18).

Some people, especially in the US, for example Agre and Harbs, believe that, in most circumstances, the unambiguous irrefutable identification of individuals without their consent is an invasion of privacy (Agre, P. & Harbs, C., 1994). Hibbert supports this view,

> "Many people are concerned about the number of organisations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being treated as just a number. Unfortunately, (Hibbert) can't offer any hope about the dehumanising effects of identifying people with numbers. " (Hibbert, 1999, p. 1).

Contrarily, a national opinion survey carried for the Columbia University in the USA in 1996 by the Equifax/Harris Information Service, claimed to show that a majority of people may be becoming more optimistic in their outlook towards privacy protection (Harris & Westin, 1996). Most people would agree that scanning should be restricted to specific situations. For example, usually it would be reasonable to expect a lender to scan the credit record of a borrower, but indiscriminate database scanning, or the scanning of data collected for some unrelated purpose, would rarely be justifiable.

4.9.5 Vehicle identification

If a card forms part of the electronic systems of a car, it might become impossible for the driver to remain anonymous or deny anything recorded on the card. The potential would exist for authorities to use this feature to supplement enforcement, surveillance and scanning (Wigan, M., 1994). A survey, commissioned by the Australian Automobile Association, concluded that many motorists thought vehicle tracking was "great for stolen cars but ... unacceptable... for stolen moments" (Motorists' views, 1996). Despite the survey's conclusion people may be becoming more tolerant of electronic identification techniques (Butler, G., 1996). A general conclusion is that smart card technology, if properly designed and implemented, may enhance both the fact, and the perception, of the consumer's ability to exercise a much greater degree of control over personal information than is the case with any comparable delivery system (Consumer privacy, 1994). Nevertheless, since the technology, perhaps desirably, may also facilitate legitimate law enforcement, the basic issues of control and trust must be addressed.

4.10 Resistance to change

A final problem might be the well-known human characteristic, "resistance to change", a characteristic that is derided by those seeking to introduce changes, but is understandable, nevertheless. If one has mastered a way of dealing with one's situation or environment it is hard work coping with change and, if no gain from the change is perceived, resistance is a logical response. It is, therefore, the task of the innovators to persuade and convince, rather than compel. Ideally, there should be some gain for those who must change. Hopefully, in most situations, users will have a choice between options, but there are already indications that the first people to use smart cards in large numbers might be beneficiaries and commuters by public transport (Lunt, P., 1995). Neither group may be considered powerful, nor will either benefit much. On the other hand the Australian Federal Bureau of Consumer Affairs takes a more optimistic view. It writes:

> "Changes in financial services are not happening overnight, and to a significant extent the success or failure of innovations is being determined by consumer demand. Most importantly, some of the new developments do have a real capacity to benefit consumers." ("Cashless society", 1995, p. 2).

4.11 Conclusions

Standards for the smart cards themselves are reasonably acceptable and mature, but standards for card operating systems and applications are still at the stage where industry groups are promoting competing solutions; consequently, interoperability issues remain unresolved. There is as yet no evidence of any fall in smart card costs. Vehicle insurance premium reductions are likely to be less than the cost of vehicle security, so a smart card supported security system will probably be incidental to other smart card advantages. It follows that improvements in the capacity and speed of smart cards are essential and there is a need for open systems so that other card advantages may be exploited. Smart cards are virtually proof against cracking by individuals, but are conceivably vulnerable to attack by well-funded organisations with world-level expertise. Biometric methods of identification have yet to meet required standards, their testing is difficult, and the test results controversial. Governments have concerns about consumer choice, consumer protection, "hot money" and "dirty money". Human rights activists may be expected vigorously to oppose invasions of privacy, but with the proper design and control, smart card technology could actually enhance individual control over privacy.

The crucial factor might be the difficulty of gaining the agreement of competitors to standardisation. If communications between devices and interoperability between systems could be achieved, the multi-application card might become a reality, a mass market emerge, and costs fall. Problems of security and identification would remain, but might be sufficiently controllable to be acceptable to the community. Standardisation is being hindered by the efforts of commercial organisations to gain competitive edge. This situation and related problems are examined in chapter five.

5 COMMERCIAL ATTITUDE & APPLICATIONS

5.1 General

This chapter continues consideration of the assumption that a probable precondition for smart cards to be used in vehicle management is their widespread general use which, in turn, probably depends on standardisation. Currently, commercial efforts to identify a business case for smart cards seem to focus on a search for competitive edge, rather than standardisation. Therefore, the likelihood is examined that an acceptable business case for some smart card system will be found and some "killer application" emerge, to provide the core of a multiple application card whose acceptance might create the environment needed for the adoption of smart cards in vehicle management. In that event, many of the organisations currently fighting for dominance might have to accept niches, whilst the industry as a whole might burgeon. Following this line of thought, having identified the "players" some possible "killer applications" are evaluated.

5.2 The smart card industry "stakeholders"

The "stakeholders" in the industry, each of whom must foresee a potential for profit, may be grouped into four categories, as follows:

- Manufacturers who endeavour to sell the technology to the next group. They include:
  - Chipmakers who have been described with the major names listed in section 2.3.
  - Card makers who embed the chip in the card and may design the card operating system. As part of this process the card maker usually supplies the chipmaker with a mask that installs most of the operating system in the chip ROM. This mask forms one of up to 15 used in chip manufacture. Major card makers are Gemplus, Schlumberger, Bull, Siemens (Infineon), Phillips, Oberthur, Orga, Datakey and Toshiba, but there are at least ten others.
  - Peripherals manufacturers who make the readers, terminals and other supporting hardware.
- System providers, who constitute the market for the first group and co-operate in order to create the market. They include:
  - Card issuers which either are, or are prepared to assume the responsibilities of, a financial institution. Cards with applications that have no financial implication, for example identification cards, need only a sponsor. Cards with financial applications, however, need an issuer who is likely to be a bank or other organisation normally responsible for supplying credit cards, debit accounts, checks and electronic tokens, but might be an insurance, transportation or telephone company. An issuer sets the card or account holder's credit limit, pays for his/her purchases, funds the free credit period and any extended credit, and displays its name on the card ("Electronic Cash", 1996).

  - Acquirers or funds clearing houses which are financial institutions that support merchants by providing a service for processing card-based transactions ("Glossary", 1999). Acquirers are actually, but not necessarily, banks, and, often, either are issuers or else control or own the issuer. For example, Mastercard and Visa, potential issuers, are each owned by a consortium of banks.
  - Organisations whose programmers personalise the card. Recall, from section 4.5.2, that personalisation is the process of taking a "generic" smart card and customising it with data that are specific to a single- or multi-application card and the individual card holder. Almost all applications require the card to be personalised. These organisations are usually hired by, and are answerable to, an issuer.
- Merchants who provide goods or services and accept payment by way of the cards.
- Holders, members of the public who are prepared to use a smart card.

Naturally, amongst these players there is discussion about who will benefit the most, and what proportion of the cost each should bear: their expectations of benefit impact upon the prospects of any potential application category.

5.3 Financial applications

5.3.1 Transactions generally

Today, almost everyone carries some sort of financial card, be it debit, credit, or stored value. Naturally this situation suggests financial applications as being candidate "killer applications" for smart cards. Discussion of some possibilities follows. Commercial transactions may be classified as either cash, or accrual, in nature. Cash transactions take place virtually instantaneously; the item purchased and the cash being exchanged simultaneously (Horngren & Harrison, 1989, p. 86). A stored value smart card application, including an electronic purse, might be used to implement a cash transaction. Accrual transactions are initiated when either an item or cash is transferred, but the reciprocal transfer that completes the transaction, occurs later. All parties to the transaction must be assured that:

- the other parties are genuine, identifiable and locatable,
- the implementing messages are correctly attributed and unaltered, and
- the confidentiality of the message contents is preserved.

In accrual transactions, smart card applications could be used to facilitate the eventual payment, to provide the essential mutual identification, and possibly to provide secure storage for any encryption keys. Transactions involving credit cards are accrual in nature.

5.3.2 Bank attitude

Before discussing the possible nature of smart card supported transactions the attitude of the trading banks, especially the US banks, will be considered. Smart cards have yet to be adopted worldwide by financial institutions because, although fearful that others will take the business, banks are wary of participation in the development of smart card systems; being concerned that the business case for their use is weak (Lunt, 1995). This caution is particularly true of the USA financial community which, being the engine driving world finance and commerce, has a global influence. A reason for the USA reluctance, advanced by many writers, is that the existing investment in an infrastructure relying on magnetic stripe cards and an elaborate communications network is too great to abandon until it truly fails (Fancher, 1996; Duffy, 1996). Whilst the existing system suffers steady losses due to fraud, the losses are not systemic and, although increasing, are not yet sufficient, in many eyes, to justify the change to smart cards (Duffy, 1996). Svigals contends that the reason that the United States lacks a realistic, smart card, credit-card, action plan is simple: the two major bank credit-card associations (Visa and Mastercard) are service companies, and derive their revenues from their investment in networks and online authorisation services. The merchant pays for each online authorisation; the fee being a 1.5 to 2 percent discount based on transaction value. In 1995 those fees amounted to US$10b (Svigals, 1996). Although Svigals does not make his opinion more explicit, his contention implies that he believes the credit card companies oppose the introduction of smart cards as electronic purses because they do not wish to lose this cash flow. If his contention is true, Visa and Mastercard seem to have adopted different strategies. Visa promotes VisaCash, an online payment system in which the smart card functions rather like an instantaneously cleared personal cheque, whilst Mastercard has purchased Mondex, a largely offline system where the smart card functions like a digital traveller's cheque. On a more optimistic note, it is possible that the introduction of financial smart card applications might be more rapid if a cheap reliable system of biometric identification could be developed and introduced.

5.3.3 Cash transactions

To evaluate the potential for smart card implemented financial transactions, it is necessary first to estimate the size of the market. A discussion of the mechanisms by which the currency might be created and controlled, and of the forms not involving smart cards, lies outside the scope of this thesis, and it should be noted that there are sceptics who think stored value cards may never be popular. For example, Bert Ely, in an article for the Cato Institute, writes:

> "...it will be much safer to hide ten US$100 bills in one's home rather than carry a US$1,000 balance on a stored-value card used frequently to make small purchases." (Ely, 1996, p. 2).

Sceptics there may be, but most authorities seem to think the electronic purse could function in the area at present employing coins and notes. A number of estimates of the total value of annual cash payments worldwide and the references upon which they are based have been relegated to Appendix 4. Suffice to say here that a reasonable estimate might be US$10t. This total may be small in value relative to that of transactions as a whole, but if, for example, smart cards were used for a major part of the transactions at present effected using cash, then almost everyone would have such a card, and their adoption for vehicle management would probably follow.

5.3.4 Electronic purse definition.

Section 2.2.1 listed stored value transactions as one of the application categories of smart cards. A smart card that provides a store of value as one of its functions is a novel financial instrument, and the financial institutions will probably be major players in its development. In section 2.2 a distinction was drawn between stored value cards and their subset, the electronic purses. Both contain spendable digital tokens, but the purse may be reloaded and is more suitable for open systems.

5.3.5 Electronic purse contenders

Given the size of the market, it is not surprising that there is the usual struggle for dominance, as evidenced by a report issued in September 1996 by SJB, a company selling data about smart cards. The report claimed that a battle was in progress between the five major potential purse card issuers, which SJB identified as Mastercard, Mondex, Visa with VisaCash using Banksys technology, CLIP and Proton (Battle, 1996, p. 1). Since Mastercard has now purchased a controlling interest in Mondex, presumably, the "big five" have become the "big four". David Jones, editor of SJB's Card Technology Today (CTT), wrote

> "Two major questions loom over the Big Five purses. Will there be serious competition from non-banks? And is there scope for an international purse?"

As to the possibility of new competition, Jones says the banks are well placed to issue the electronic purse, for four main reasons.

> "First, consumers already look to banks to supply payment instruments. Secondly, retailers already look to banks to process card-based transactions. Thirdly, banks can make use of their international networks (e.g., Europay, MasterCard and Visa) and their national networks for settling purse transactions. And finally, banks have, or are on the point of having, the necessary smart card technology in place."

However, CTT, whilst it did not pursue the idea of an international version, elaborated on the possibility of competition by pointing out that:

- there was no reason why only banks should issue a purse,
- phone companies already issue stored value cards,
- card usage could be widened to include many types of small retailer, and
- mass transit operators are active in the field, since transport operator Creative Star is running one of the world's biggest purse schemes in HongKong (see sections 5.9.2 and 7.6.6).

An article in the Economist in April 1997 considered the question indirectly. By then Proton, still the largest distributor of purse cards, had made a deal with American Express; no minnow by card issuer standards, but nevertheless not large enough to guarantee Proton independence. The article hinted at an eventual alliance between Proton and Visa ("Electronic money", 1997 April 26). Four years on, there is still no report of any such alliance but if it did eventuate the outcome would see Mastercard (Mondex) competing with Visa (Proton) and leave CLIP (sponsored by Europay) unlikely to survive outside Europe. The possibility does not augur well for an international purse except within Europe, where the introduction of the eurodollar might nullify one of the arguments for a pan-European purse. In short, the prospects for a smart card supported cash transaction mechanism are not yet favourable.

5.3.6 Accrual transactions

The second financial area in which smart cards might make a major contribution is in electronically conducted accrual transactions, or e-commerce. Apart from foreign exchange transfers or "hot money", which will be briefly defined and then excluded from the discussion, if one accepts the estimates formulated in Appendix 4, e-commerce currently probably forms less than one percent of total world commerce. There are many definitions of e-commerce but electronic monetary transfers may be grouped into three broad sectors:

- "hot money" flows,
- e-commerce or business to business (b2b) payments, and
- e-tailing, e-shopping or business to consumer (b2c) payments.

These are now considered in more detail.

5.3.7 Hot money

"Hot money" has already been discussed in section 4.8.2, and is valued in hundreds of trillions of US dollars. At US$2t per day, US$700t per year may be a reasonable annual estimate. It is true that the volume of electronic transactions using dedicated communication links controlled by the financial institutions is gigantic, but in this activity only a relatively small number of financiers are involved, and, even if smart cards were used, most people would be unaware of that fact. Most authorities, when discussing e-commerce, exclude "hot money".

5.3.8 E-commerce

Electronically conducted accrual transactions between major organisations (the most common meaning of the term e-commerce) are valued merely in billions of US dollars. Many writers include Internet shopping in this sector, but a separate discussion of that category has been deferred to the next paragraph. Detail of estimates of the total and the references upon which they are based have again been relegated to Appendix 4 but a plausible estimate is probably about US$210b. To obtain some sense of proportion this estimate can be contrasted with the world's GDP of about US$35t or total share-market capitalisation of US$32t. The wide variation is probably a consequence of differing definitions, but the market is certainly growing. In this type of e-commerce, authentication might be the most useful function of smart cards, because they are capable of delivering all needed controlled and traceable accesses; although it is true that money flows could probably continue by traditional channels. Despite that likelihood, there is a growing body of opinion that the need for identification of all parties to an e-commerce transaction could 'drive' the introduction of smart cards.

5.3.9 E-tailing

Internet shopping, the third sector (sometimes referred to as e-tailing), is made up of individual buyers who purchase using the Internet and usually buy small items such as computer programs, magazine articles, and CD-ROMs, and, at least in the USA, effect payment with credit cards. Currently, this market is smaller than the market for the "purse" and, until recently, could be measured in millions of US dollars. Yet again estimates of its current total and supporting references have been relegated to Appendix 4, but a reasonable figure might be US$10b. From the perspective illustrated in Figure 4 it may be concluded that the claims sometimes made that e-shopping is about to change the world is premature. Exacerbating the problems of e-shopping are those of handling micropayments, which are briefly discussed in Section 7.6. Finally, it should be noted that even if the e-shopping total is smaller than predicted, individual purchases over the Internet could have implications for those states, or political entities, that depend on sales taxes for revenue.

Since it is easy to overlook the great difference in scale from global financial flows, to world commerce, to e-commerce, to e-shopping, the following diagram attempts to put these figures in perspective. It is not to scale. All figures are in US$

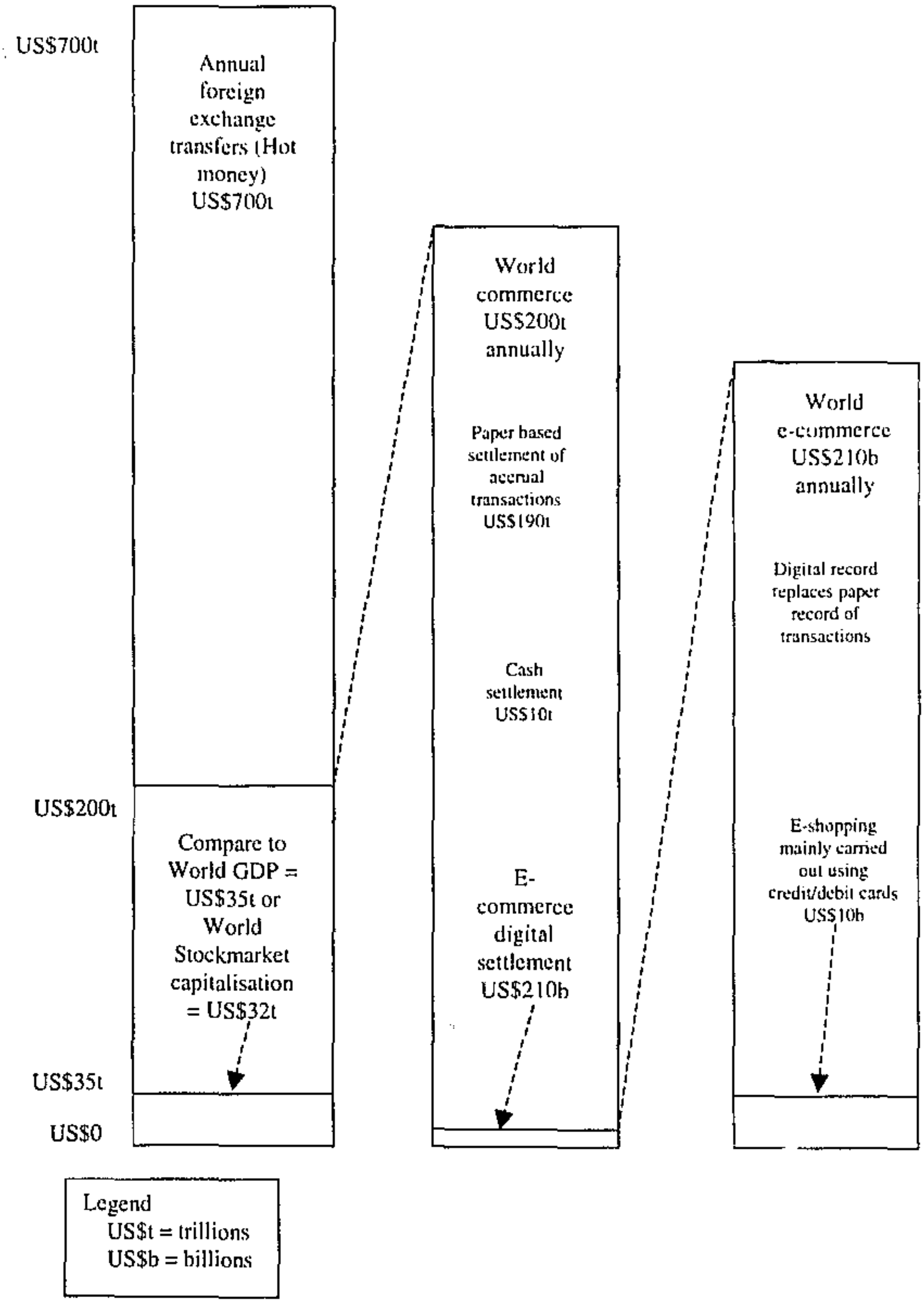

US$700t
Annual foreign exchange transfers (Hot money) US$700t
US$200t
Compare to World GDP = US$35t or World Stockmarket capitalisation = US$32t
US$35t
US$0
World commerce US$200t annually
Paper based settlement of accrual transactions US$190t
Cash settlement US$10t
E-commerce digital settlement US$210b
World e-commerce US$210b annually
Digital record replaces paper record of transactions
E-shopping mainly carried out using credit/debit cards US$10b
Legend
US$t = trillions
US$b = billions

Figure 4: World finance and commerce in perspective

5.3.10 Security problems with e-shopping

Traders are believed to be wary about making major purchases and reluctant to pass their authorising numbers across an Internet that they may not regard as secure: they have good reason for their caution. The description of a fairly recent scam shows how, using stolen or irregularly acquired credit card numbers, a group stole US$47m from members of the US public. The amount stolen from any one person was small but, according to the report, both Visa and Mastercard made a profit from the scam (Wallich, 1999; Faughnan, 1999). In 1996 Walter Wriston formerly CEO of Citibank believed that the major impediment to the expansion of electronic payments is the security of the Internet and, in particular, the US Government determination that it must be able to decipher all ciphers (Wriston, 1996), but two years later Charles Goldfinger, Chairman of the European Financial Issues Working Group, believed there to be a growing consensus that secure payment could be achieved by a combination of PKI and digital signatures (Goldfinger, 1998). The US may have been persuaded because it now permits the use and export of "unbreakable" encryption schemes. Theoretical solutions designed to overcome security fears are being advanced in most developed countries, and small schemes are being implemented. The solutions range from the use of trusted third parties, to encrypted digital numbers representing cash that are purchased from an issuer who is bound to redeem them when they are presented. The schemes depend on reliable identification, and probably any of the candidate standard smart card schemes discussed in section 4.4 (Multos, Javacard, and Windows for smart cards) could provide this feature if the business community could agree on one of them.

5.3.11 Summary

The electronic purse possibility appears to be stalled in a competitive tug-of-war and because the business case is weak, but e-commerce is growing rapidly, and if the business community accepted smart card systems as a facilitating mechanism, smart cards could become as ubiquitous within that community as photocopiers are now. For the general public, that situation would be matched only if e-shopping equalled the growth of e-commerce, which it has yet to do. As with the electronic purse, the acceptance of smart card based system(s) would imply public familiarity with the cards and the existence of the infrastructure needed to support them, and their adoption for vehicle management would probably follow.

5.4 Telecommunications

In many countries the telecommunications industry, is directly owned by the Government and, even privately owned telecommunication companies, known as telcos, are heavily regulated. There are logical reasons for this situation. Telecommunications:

- has a substantial direct effect on the national economy,
- by its nature, tends to be monopolistic,
- requires global, let alone national, standardisation,
- uses a limited public resource (the frequency spectrum), and
- requires an enormous capital investment in infrastructure.

The telecommunications industry is already the largest user of smart cards, and has experience with their use both in cellular telephones and in payphones. Furthermore, there is an increasing convergence between the computing and telecommunications industries. Therefore, telecommunications would seem to be an industry likely to produce a "killer application" that might form the core to which other applications could be added. At first glance SIM cards might be thought to be the most promising possible "killer application", because they are used to manage both money and communications, and more SIM cards have been put into use than any other true smart card. A discussion of possible reasons why this has not happened is deferred until chapter seven.

5.5 Oil companies.

Oil companies have always endeavoured to persuade their outlets to make better use of their sites by offering services in addition to the dispensation of fuel, oil and lubricants, and, in particular, payment by credit, or debit, fuel cards. Although the companies have a substantial investment in the databases created from the data obtained from fuel cards, if vehicles generally included a smart card system with a stored value application, the cost of obtaining on-line authorisation for purchases could be reduced. Further, if motorists habitually used smart cards to purchase petrol and other items at petrol stations, the cards could become an extended source of marketing information (Dick, 1995). However, control of the data might move from the oil company to the car owner. Accordingly, oil companies might be ambivalent about any moves to establish such systems. Each company may be expected to favour a proprietary system that "locks in" its customers and, thus, the inevitable "conflict of interest" obstacle to standardisation might reappear. On 14th March 1997, in the UK, in an apparent effort to circumvent customer resistance to this strategy, the Shell Oil Company launched "Shell Smart", a cooperative effort by Shell and a number of substantial companies in different fields. The companies were:

- Commercial Union
- Dixons
- Hilton Hotels
- John Menzies
- The Link
- RAC
- Shell
- Vision Express
- Victoria Wines.

No other oil company participated ("InTouch", 1998). Even this scheme is likely to encounter customer resistance because, for example, the customer who likes Shell petrol might not like Victoria wines.

5.6 Major retailers

Cooperative, departmental and mail order retailers, world wide, are seeking to encourage customer "loyalty". Supermarkets, which usually provide free parking for their customers, might be keen to promote a smart card parking system if it would enable them to identify and reward their better customers (Duffy, 1996). The customers, themselves, would probably prefer a card that was valid at any supermarket of their choice; a conflict of motivation likely to delay the introduction of any scheme.

5.7 Entertainment

Smart cards could be used to authorise viewing of in-house entertainment, such as pay TV, in much the same way as for access to public transport, although the possibility of petty fraud is greater, since the holder is likely to have undisturbed access to the reader (Seidman, 1994). An advantage from the entertainment provider's point of view is that, given an appropriate connection, the smart card could be either reloaded or nullified without the need to visit the in-house terminal. The payment scheme eventually chosen might depend more on the outcome of competition between telecommunication companies than that between smart card issuers; a choice that might not be made for some time.

5.8 Local authorities

Local authorities, such as city councils and shires, are unlikely to agree upon any single scheme, and might be expected to be cautious about pioneering any high technology solution, but have at least two potential, vehicle related, smart card applications.

- The control of congestion and pollution. For example, as described in section 3.2, in Singapore smart cards are used to support a system that imposes a fee upon the drivers of vehicles that enter a designated central area.
- The control of parking. Luk has suggested a two-stage strategy for moving towards a smart card-based system. Civic authorities could first institute a magnetic-stripe, disposable-card system, and after a period, perhaps three years, upgrade it to a reloadable, smart card system. He believes that public acceptance, rather than technical difficulties or the need to raise revenue, will be the controlling factor. In discussing problems, he points out that an infrastructure would need to be established to sell the cards and recharge them, and that a funds clearing house would be required, and claims that banking institutions are reluctant to be involved in low value transactions such as phone calls or parking (Luk, 1995, p. 11). That might be so at present, but if smart card systems began to be installed nationwide, the banks would be loath to let the business go to others.

In Perth, as elsewhere, the city fathers are waiting for the bandwagon to move before jumping aboard. Two major prerequisites are the widespread adoption of electronic purses and standardisation (preferably international) of the technology for parking.

5.9 Federal and State Governments.

Governments, worldwide, are investigating the possibility of electronic regulation and delivery of services (especially social services), and the potential for smart card systems in applications of this nature (see section 7.5.5). All these possibilities might have an indirect, but only road pricing a direct, effect on vehicle management.

5.9.1 Road pricing

Road pricing is under consideration by many national and regional governments (Harrop, 1994). Roads are a national investment, but the return on the investment is uncertain, and the methods of collecting it, currently either through general taxation or through fuel taxes, are controversial ("Options", 1966). Recognising that road pricing is an emotive, as much as logical, issue, Governments are proceeding cautiously. A call for submissions from the NZ Ministry of Transport seems to indicate that government support for a road pricing will not be forthcoming unless the alternatives become insupportable ("Options", 1996). If benefits, such as better funding for road construction, reduced congestion and pollution, and increased safety, can be demonstrated, governments might adopt a more positive attitude. If that happens, ease of use may dictate an automatic toll system, and give a boost to the installation of smart cards in vehicles (Harrop, 1994). As described in section 3.2, and demonstrated by the Singapore ERP, a technical solution to the problem of efficiently collecting road tolls seems to be within reach. A non-technical problem is the difficulty of standardising both charging and charge collection systems (Electronic toll collection, 1997).

5.9.2 Public Transport Ticketing

A promising commercial area in which smart cards might make a substantial, initial impact is transportation, since contactless cards might provide a convenient way of authorising access to the transport medium, and a rapid method of payment. From the transport operator's point of view this rapidity is highly desirable for its own sake, but, in addition, the operator would be able to acquire valuable statistics about the passengers. The major disadvantage of contactless smart cards is their cost. A secondary problem is that current systems are vulnerable to individual petty fraud, although the possibility of a systemic fraud appears small. Major schemes are being conducted in many parts of the world, of which the largest is in HongKong. In Australia, Transcard, a multi-function, reloadable, stored value, transportation access card is being trialed in Sydney. A small scheme was first implemented in the suburb of St Mary's, and then, in 1996, expanded into western Sydney generally. Consumer research conducted by McNair, indicated that although users found contactless cards convenient to use and readily acceptable on buses, this was not true of shopkeepers, who failed to provide vending devices. Consequently, card usage has failed to expand to any marked degree. If expanded acceptance does occur, the card issuers will want to exploit the user base and add other applications, which might put pressure in the financial institutions either to develop contact cards, or to exploit the contact interface of a dual interface option. In South Korea the Pusan Bank plans a large (1 million cards and 10,000 terminals) pilot scheme and proposes to use a dual interface card in this way ("South Korea bank", 2000). If these and other schemes prove successful, in the future a symbiosis between banks and transportation operators might develop.

5.9.3 Health.

At least two possibilities exist for the application of smart cards in health. First, a card could be used to store its holder's individual health record, and the cards of a population of patients then analysed to produce a reference database. There is a growing need to store, retrieve and analyse, large volumes of data because the number of tests available to medical professionals is increasing rapidly. A smart card system might meet the requirement efficiently (Hannan, 1994). A smart card supported health record system has been implemented in France. The concept is analogous to that common in business, where not only are records kept of transactions and analysed to provide a view of the situation of the business, but, in addition, industry associations keep aggregated records of the situations of their members, so that any member is able to see how it is performing in relation to the other members. Second, since health administration commonly involves benefits and other public contributions, administrative, as opposed to medical, detail could be stored on the card. Germany has introduced this type of system (Duffy, 1996). If the possibility of storing either medical or administrative information is fully exploited, smart cards are likely to become more familiar to the general public.

5.9.4 Welfare

In several states in the USA, biometrics, sometimes in conjunction with smart cards, have already been introduced as an authentication device to prevent fraud (Campbell & Alyea, 2000). Several authorities have suggested an extension of this system to use the smart card as an electronic purse, but the suggestion does not yet appear to have been tried. Nevertheless, it seems a likely candidate for application development, since the number of cardholders would be fairly large and individual holders would have difficulty in pressing any objections. In September, 1998, the Asia Pacific Smart Card Forum, whose members include most leading Australian smart card companies, wrote to four Federal Ministers complaining about the delay by Centrelink in deploying smart card delivery mechanisms ("Smart-card makers", 1998). The Government response has not been made public (see also section 7.5.5).

5.10 Conclusions

In the discussion of possible applications, the requirement of the holders has been considered only as a factor to be taken into consideration by the other players. Holders would probably like a multi-application card to reduce the number of cards they must carry, and the ability to choose the applications on their cards. In particular they might wish to have debit, credit and electronic purse facilities on the one card. This may cause conflicts as to the security required for each application. For example, no existing card could support both public and symmetric key cryptography. From the acquirer's point of view cost justification of this combination is marginal. There seems little chance of making profits until a "critical mass" of merchants with compatible readers exists. According to the UK Smart Card Club, experience has shown that banks and retailers do not negotiate successfully on an industry-to-industry basis. Thus there is a conflict between, on the one hand, the open, multi-application vision of the banks and holders and, on the other, the desire of the merchants to capture the "loyalty" of their customers ("In Touch", 1998). The "players" in the smart card game must each see an opportunity to benefit. As always, commercial factors will eventually prevail over technology and Government fears. Once the manoeuvring and negotiation to achieve mutually acceptable positions is over, investment in smart card applications may increase and a "killer application" emerge. In that eventuality other applications may scramble to attach themselves to the same card to form a multi-application system. When some "critical mass" is reached the much predicted explosion in card use might occur.

6 SPECIFIC INVESTIGATIONS

6.1 General

Some questions could not be answered by reference to the literature. No vehicle management system appeared to have been analysed to determine what rewritable storage might be needed, and although the potential to control the operation and security of a vehicle using a smart card as a token was obvious, no device to demonstrate the potential has been constructed to date. No information was available as to owner and driver attitudes to light vehicle management and neither was there any report of what they might pay. Therefore, to clarify these matters, specific investigations were undertaken.

6.2 Non-volatile rewritable memory estimation

A set of data flow diagrams was prepared to enable the estimation of the memory requirement for a smart card supported vehicle management system. These diagrams follow. A description of the required data stores forms part of the system repository that is at Appendix 5.

The system modelled by the diagrams is fairly comprehensive and assumes the vehicle is fitted with a transceiver enabling external entities to extract data (and, perhaps, even cash) from the smart card without the need for physical contact or stopping. This electronic purse feature would be useful for toll payments as well as regulation, since cash could be added at ATMs; and, if banks and authorities provided the appropriate facilities, it could be used for petrol purchases and parking charges. The model incorporates a provision for the driver to input a usage code to identify the purpose of the journey for usage control. Security could be either two-factor (card and password) or better (card and template derived from a biometric feature). The arming code so derived could be made a necessary input for the operation of any/all of the 10 to 20 microcontrollers in a modern car, and since these devices control the engine, the gearbox, brakes and many other features of the car, bypassing all of them to steal the car would be very difficult.

The smart card processes proposed in the model are in six groups, namely:

- enrolment,
- driver identification,
- data transmission,
- sensor polling,
- vehicle management, and
- data extraction.

Enrolment enables all the external entities to be identified on the smart card and the extent of their authority, rights and obligations, defined. In an ideal design the card might be a dual interface card, with the authentication of the driver provided via the contactless interface, and all other detail via the contact option. With such a design, no external reader would be needed to provide access, whilst the other functions could be supported by a securely located card. However, if the card incorporated an electronic purse, or other payment function, the current misgivings of the financial institutions about the security of contactless interfaces would have to be overcome. In the modelled system, vehicle activation occurs when an authorised driver supplies the correct authorisation and a usage code, or when the owner activates the vehicle in valet mode for servicing. Interaction with external authorities, or merchants, is supported, and a process can personalise the vehicle to suit the driver and control the speed. Sensor readings would be repeatedly polled and stored in a cyclic queue, and finally, the owner could extract periodically, the data stored on the smart card and obtain a report of starts, usage, payments and specified sensor records.

SMART CARD VEHICLE PROJECT

CONTEXT DIAGRAM

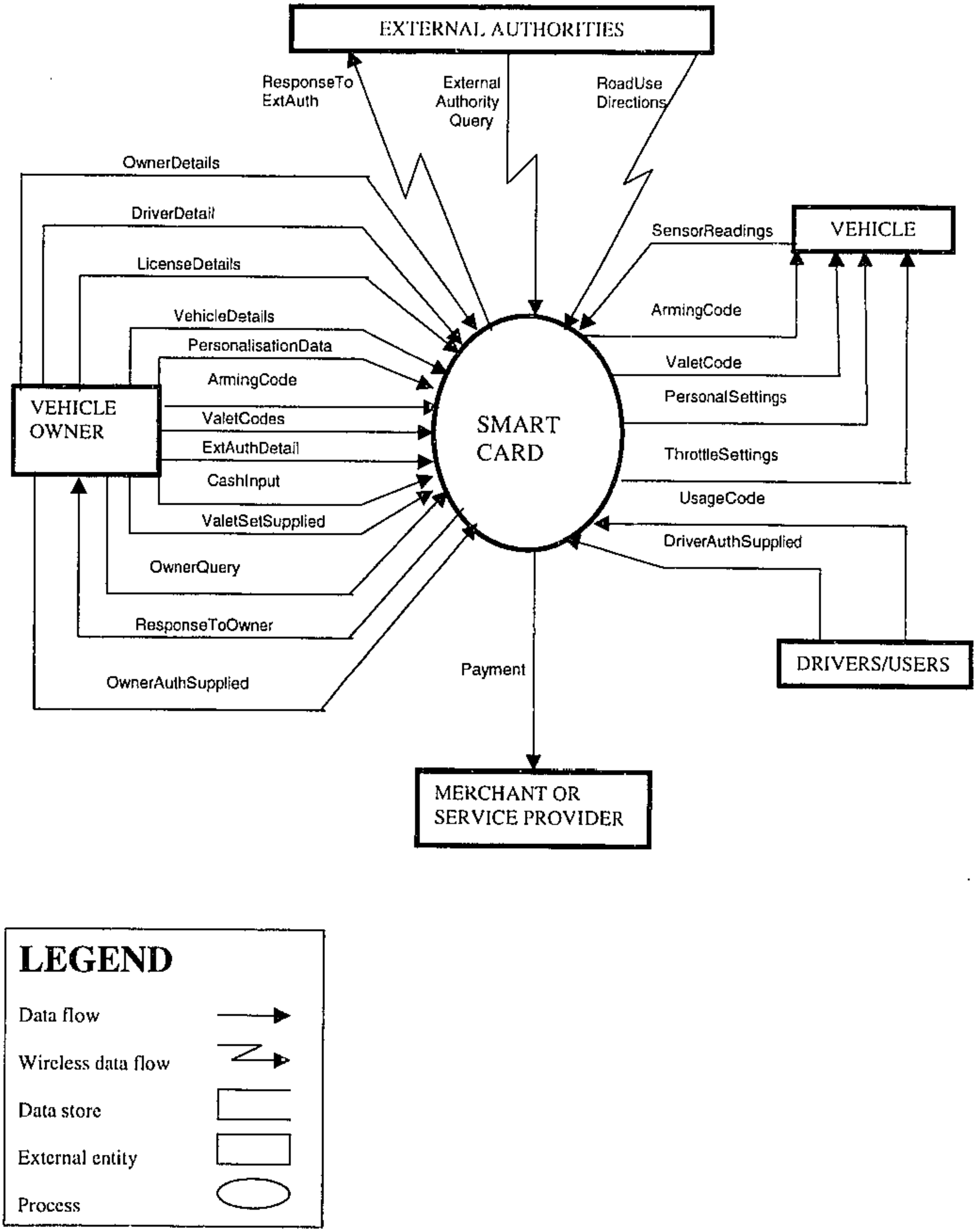
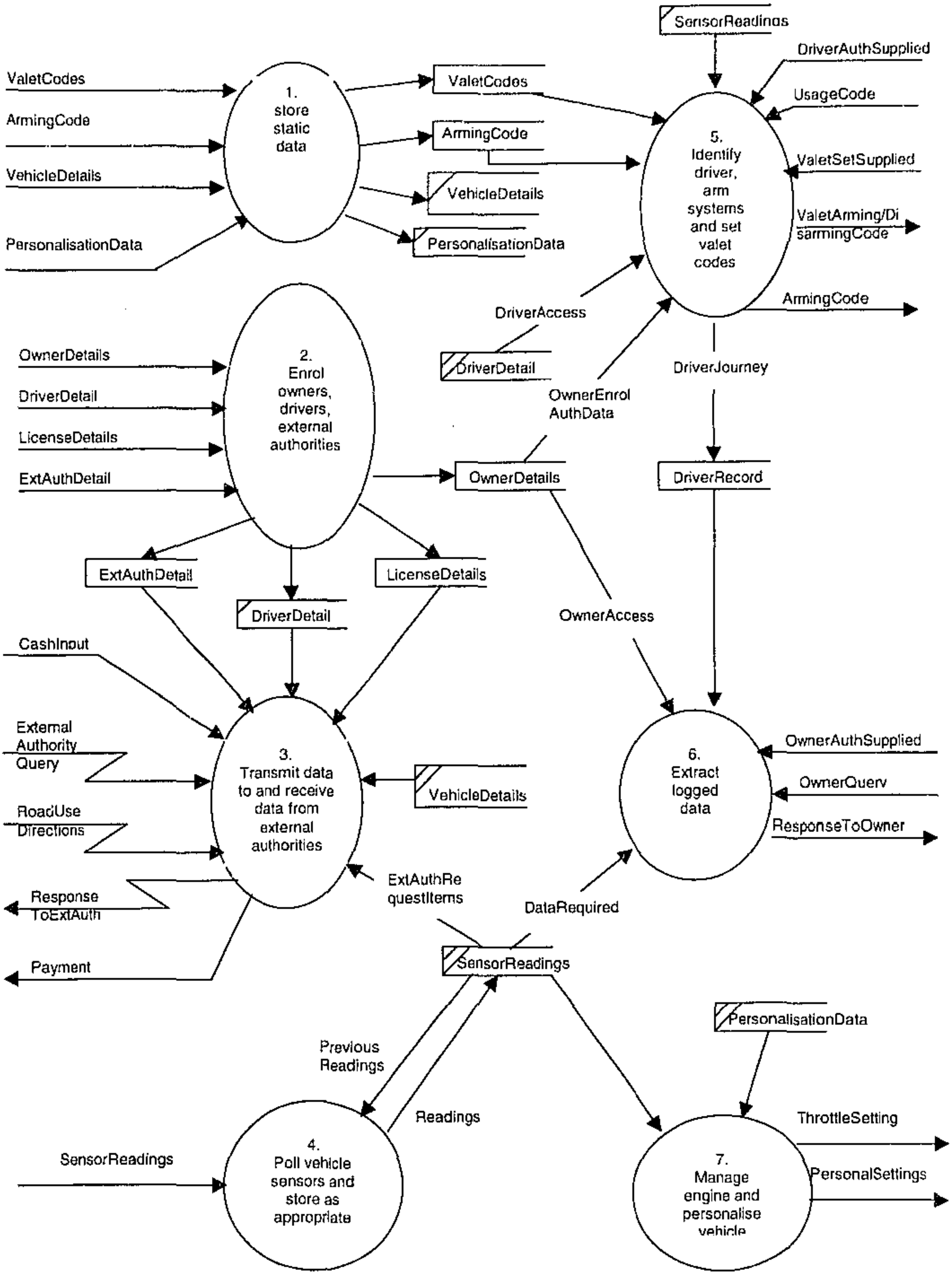


Figure 5

LEVEL 0 DIAGRAM



Note: Data flows that are identical to the stores in which they originate or terminate are not labelled and those that are identical have the same name even when appearing in different places (Hawryszkiewycz, 1998, p. 164)

Figure 6

DIAGRAM 2

Enroll owner drivers & external authorities

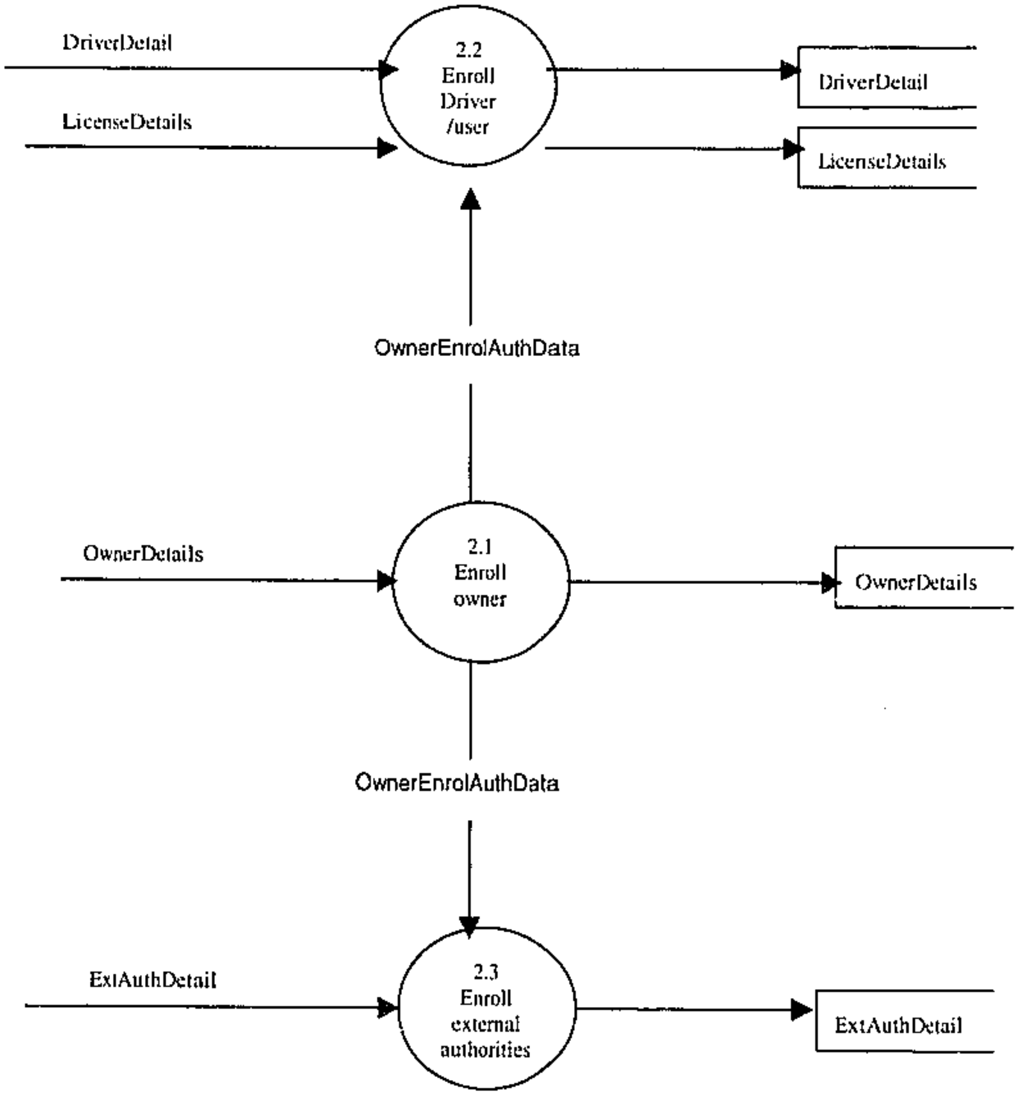
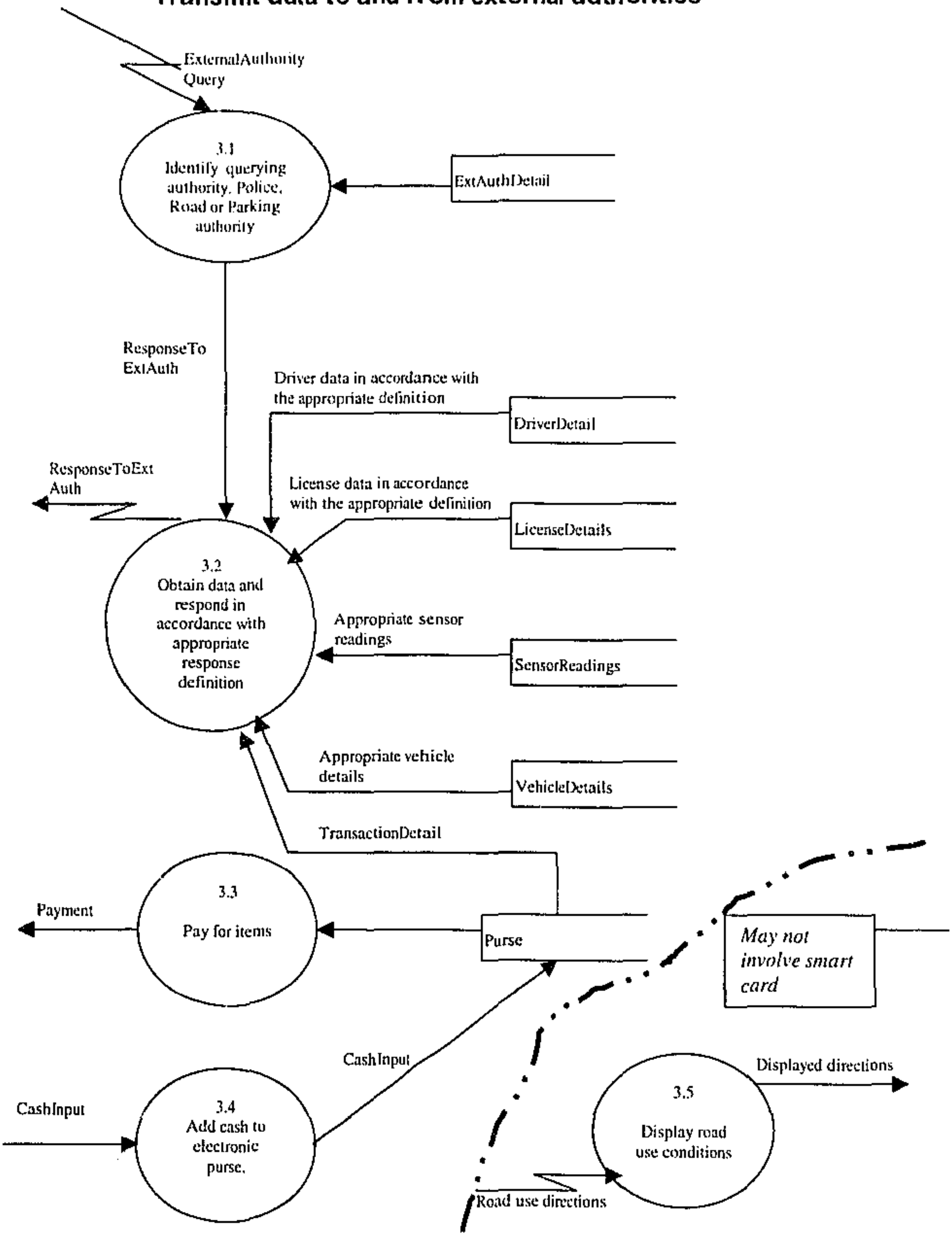


Figure 7

DIAGRAM 3

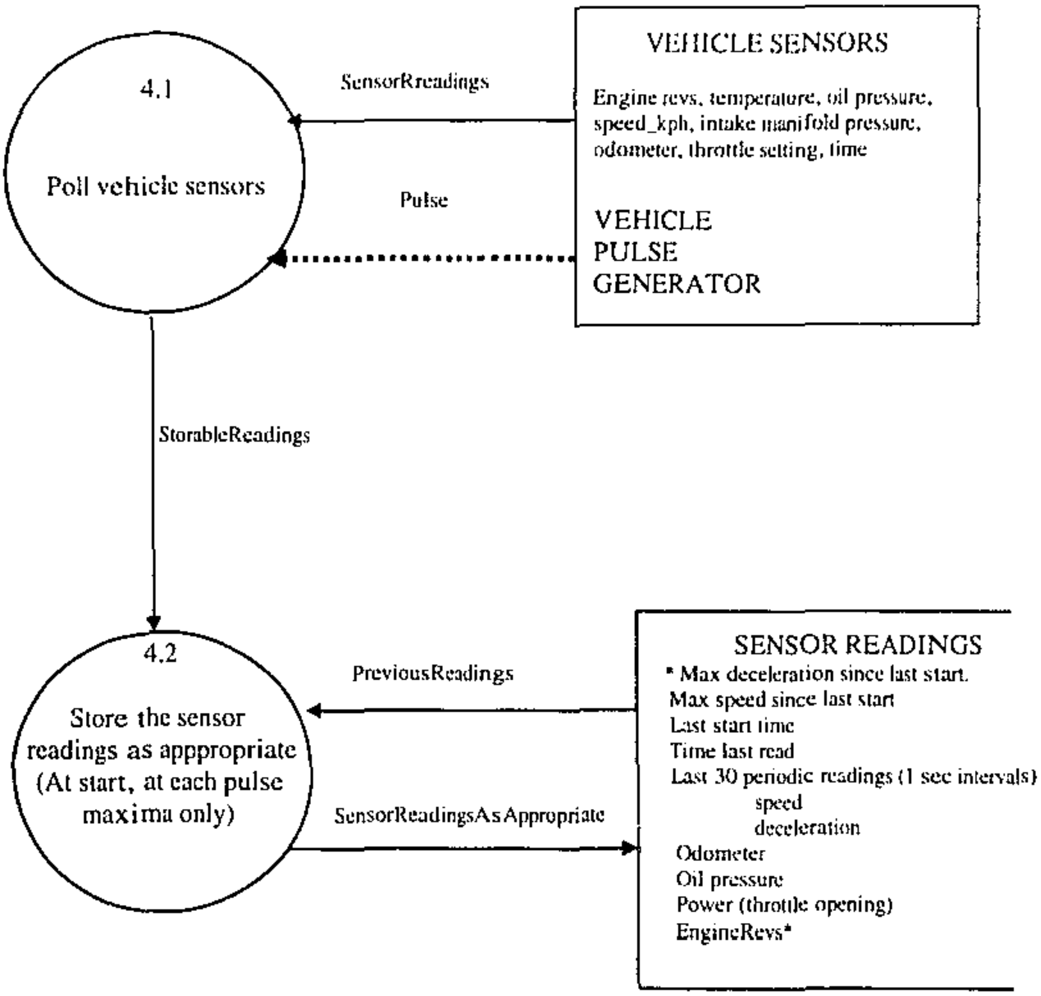
Transmit data to and from external authorities


ExternalAuthority Query
3.1 Identify querying authority. Police, Road or Parking authority
ExtAuthDetail
ResponseTo ExtAuth
Driver data in accordance with the appropriate definition
DriverDetail
ResponseToExt Auth
License data in accordance with the appropriate definition
LicenseDetails
3.2 Obtain data and respond in accordance with appropriate response definition
Appropriate sensor readings
SensorReadings
Appropriate vehicle details
VehicleDetails
TransactionDetail
Payment
3.3 Pay for items
Purse
May not involve smart card
CashInput
CashInput
3.4 Add cash to electronic purse.
Displayed directions
3.5 Display road use conditions
Road use directions

Note: Five data stores from Level 0 have been repeated here for clarity because the extracted data depends on the ResponseDefinition.

Figure 8

DIAGRAM 4
Poll vehicle sensors


4.1
Poll vehicle sensors
SensorRreadings
Pulse
VEHICLE SENSORS
Engine revs, temperature, oil pressure, speed_kph, intake manifold pressure, odometer, throttle setting, time
VEHICLE
PULSE
GENERATOR
StorableReadings
4.2
Store the sensor readings as appropriate (At start, at each pulse maxima only)
PreviousReadings
SensorReadingsAsAppropriate
SENSOR READINGS
* Max deceleration since last start.
Max speed since last start
Last start time
Time last read
Last 30 periodic readings (1 sec intervals)
speed
deceleration
Odometer
Oil pressure
Power (throttle opening)
EngineRevs*

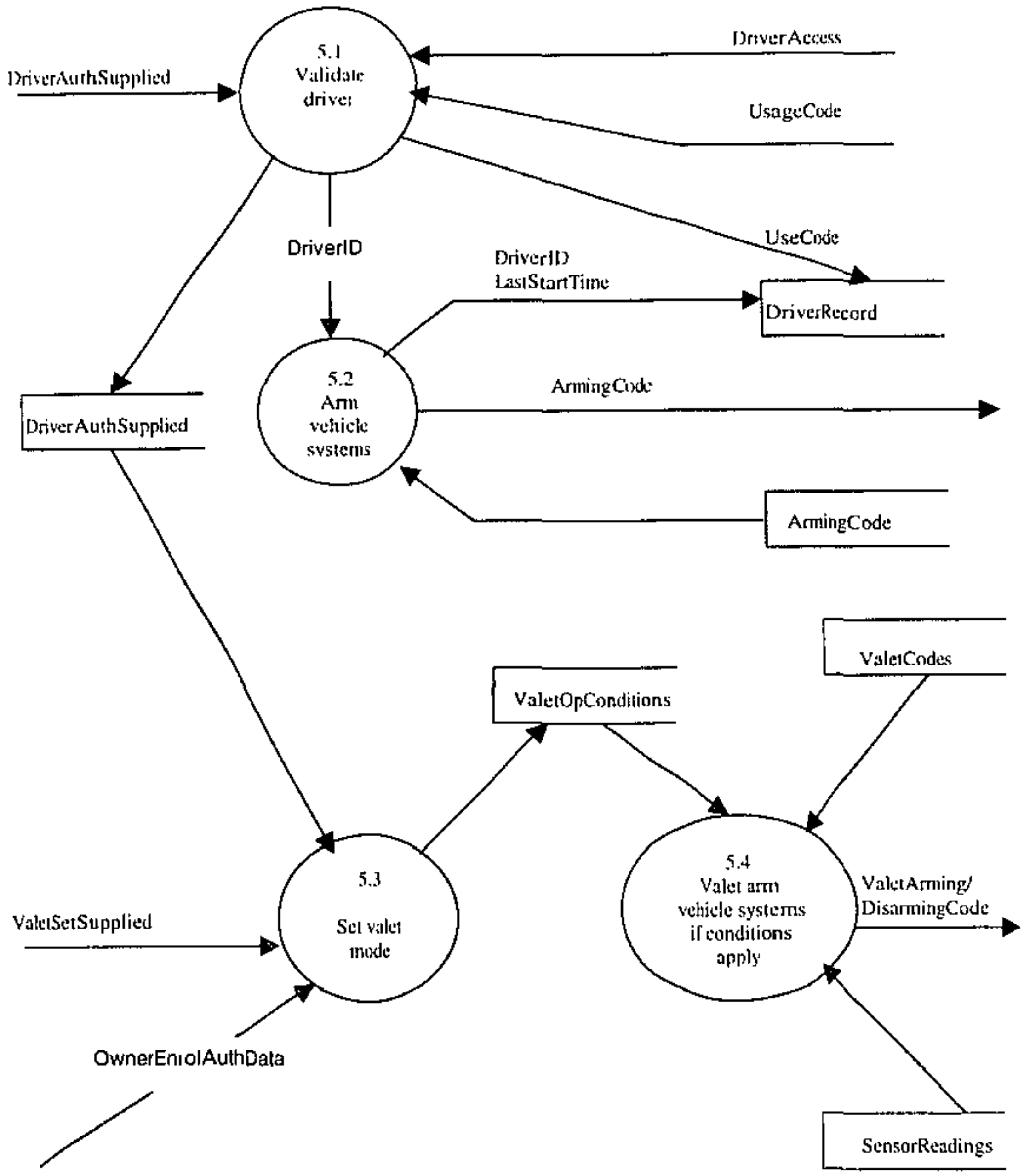
Note 1. External entity VEHICLE from the Context Diagram has been expanded here to show relevant sensors and items.

Note 2. Data store "SensorReadings" from Level 0 has been expanded to indicate relevant readings.

Figure 9

DIAGRAM 5

Identify driver



Notes:

1. Data flow "DriverJourney" to data store "DriverRecord" has been expanded into its elements:

UseCode
DriverID
LastStartTime

2. Valet mode is a state in which the owner has specified limits for date, speed and distance travelled

Figure 10

DIAGRAM 6
Extract logged data

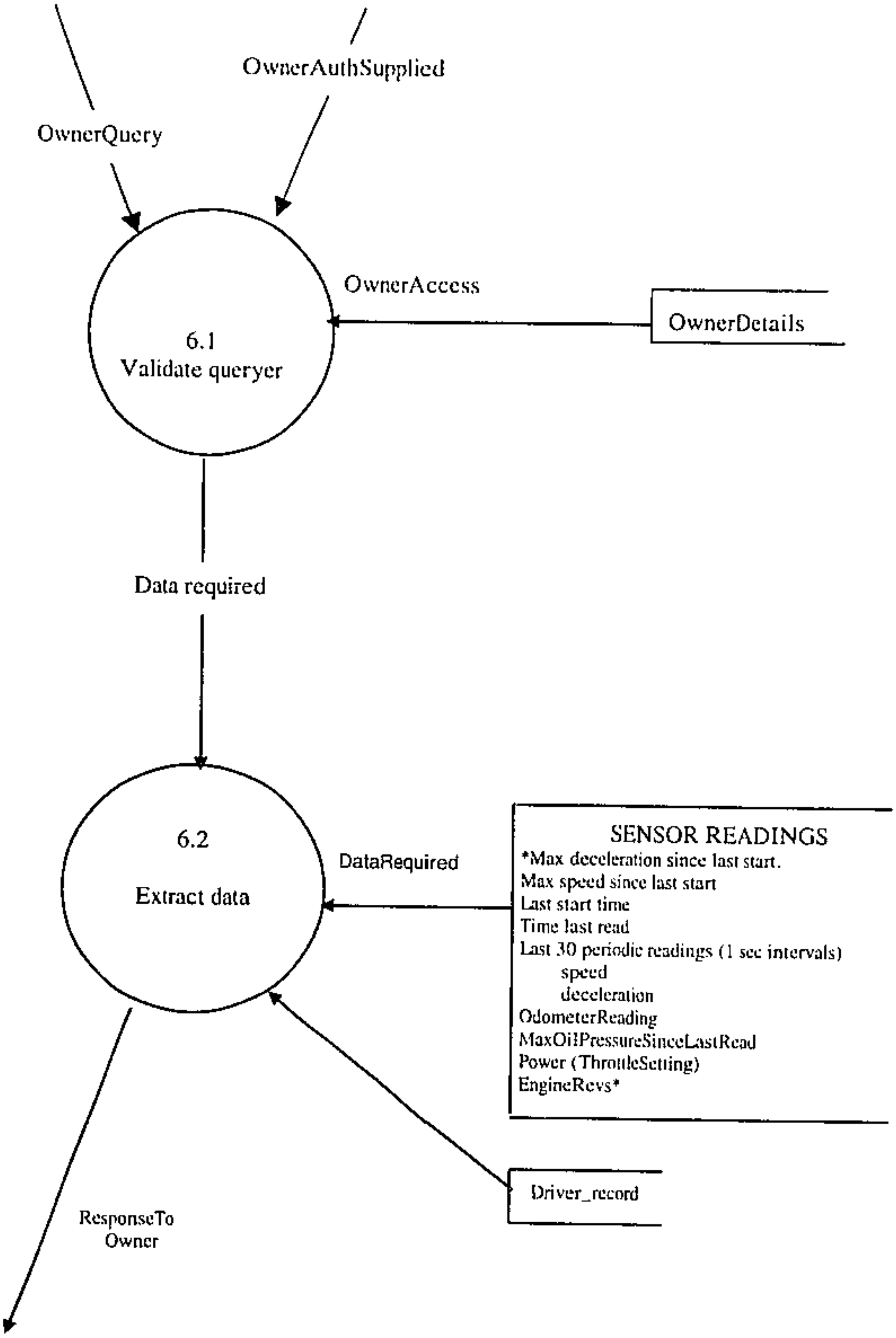
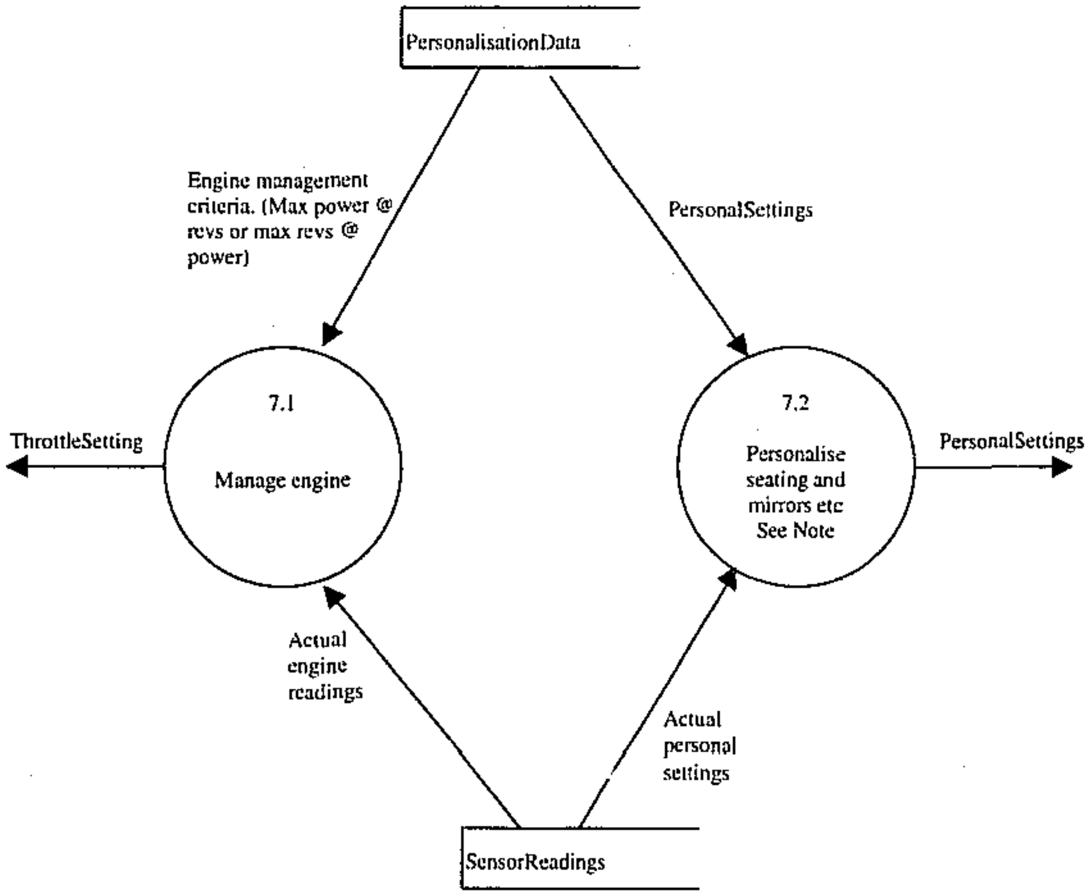


Figure 11

DIAGRAM 7

Manage engine and personalise data



Note: The owner would dictate the personalisation settings. The driver could negotiate with the owner

Figure 12

The data flow diagrams and the system repository (Appendix 5) that supports them, show that existing normal smart cards with 8 bit processors and 8K of EEPROM would be inadequate to provide all or even most of the desired applications. The "data stores" section of the repository shows an estimated initial requirement to store over 2K of data; therefore, assuming a factor of three as an allowance for expansion, the entire 8K could be used for data. Use of a factor of three is common in other engineering disciplines: for example, the Marks Standard Handbook for Mechanical Engineers proposes a figure between 1.5 and 4 depending on the degree of uncertainty (MacGregor, 1967). The object code of the program at Appendix 8, to compare a stored codeword to a supplied word, required 338 bytes, some of which was used for offsets and other constants. However, at least 200 bytes was required for the basic process of getting a data item, comparing it to a stored item and responding appropriately. Using this figure for a comparison as a yardstick, the 19 processes envisaged in the model, have been estimated to require an additional 9600 bytes (rounded to 10K) of memory. Estimates for each process, including stacks and queues, have been shown with the process descriptions in the System Repository at Appendix 5. The estimate is lent additional plausibility by figures from a paper recently presented to the CARDIS 2000 conference. Here the authors showed that the cardlets for synthetic benchmark handlers, each of which considered four kinds of Application Programming Data Unit (APDU), required from 2-to 4.5K bytes depending on the smart card used (Castella-Roca, Domingo-Ferrar & Planes, 2000). To the requirement for storage space for vehicle management processes and data stores, must be added space for other applications. A multi-application card would require an interface between the applications and the chip instruction set, which could take the form of an operating system such as MULTOS, or an application programming interface, such as the Java API, superimposed on any of a range of proprietary operating systems.

In tabular form:

Table 5: Card memory requirement

Data	8K
Processes	10K
Other applications	8K
Interface	2K
Total	**28K**

A conclusion is that even current 16-bit smart cards could not support the comprehensive system modelled. However, although the required memory is not yet provided by any commercially available card, the manufacture of such a card is within the technical potential of today's manufacturers.

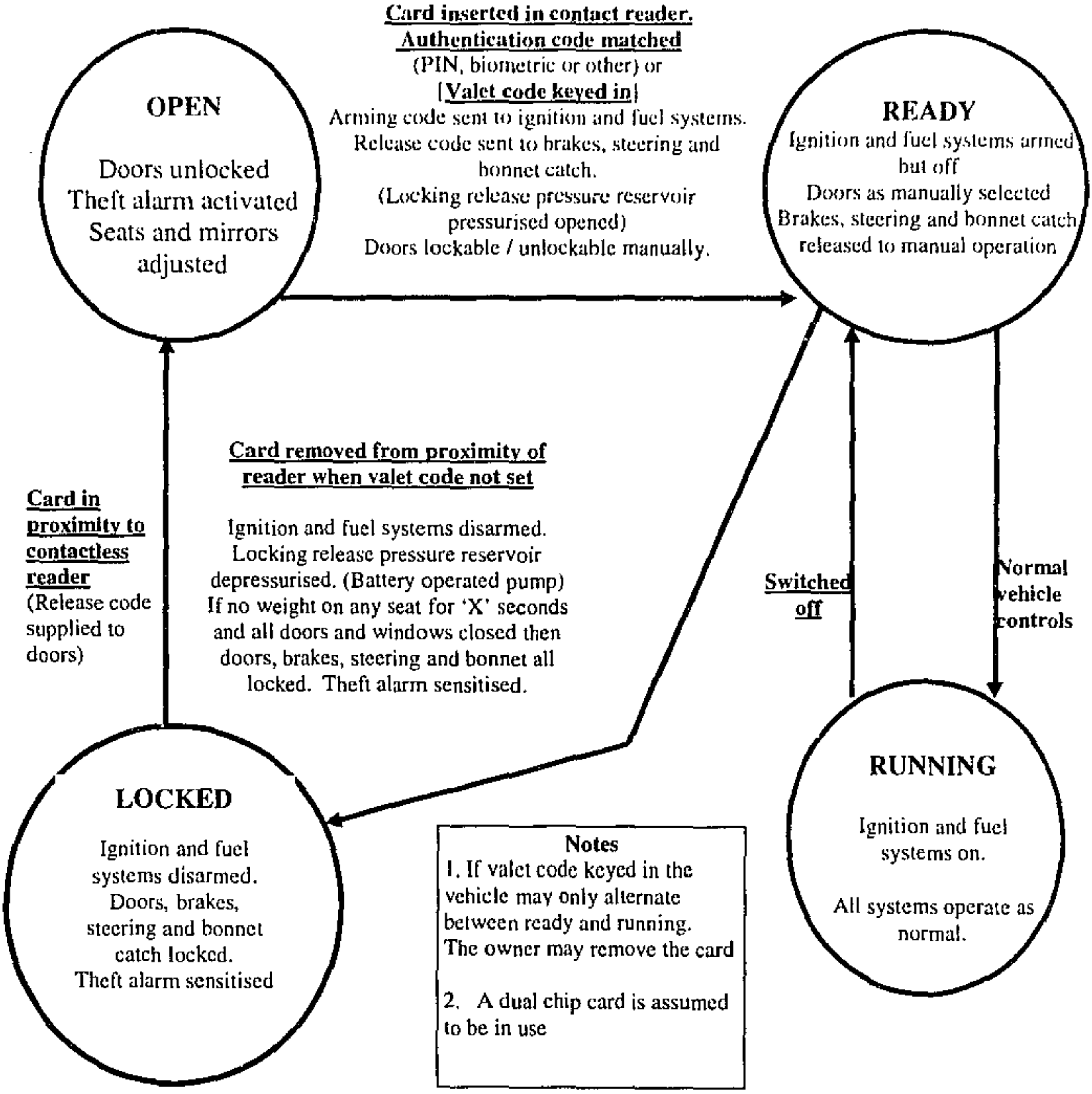
6.3 Vehicle Fleet Manager Opinions

As determined in chapter one, about ten percent of Australia's light vehicles are fleet owned. To ascertain fleet manager opinions, the questionnaire at Appendix 6 was sent to the managers of what were believed to be five of the biggest vehicle fleets in WA, eliciting responses that proved to be almost identical. In each case the present system relies on data obtained as a result of purchases made with a magnetic stripe fuel card. The static detail on the card, the amount of the purchase, and the odometer reading as advised by the driver, are recorded by the petrol station, the information is assembled centrally by the oil company that issued the card, and a periodic report is sent to the fleet manager. The canvassed managers felt that the system was reasonably satisfactory; particularly, if the same driver customarily drove the vehicle. There was occasionally a problem with defect reporting when the vehicle was driven by a number of different drivers, and managers would have welcomed more information. The main objection to the available alternative automatic logging systems was their cost.

6.4 Security and a Simulation

In chapter three potential vehicle security was described under the headings of perimeter security, alarms and immobilisers, multi-point immobilisation and aids to recovery. Apart from a possible contribution to better locking, a smart card system could do little to improve perimeter strength. since this is mainly a function of materials and manufacture, but it might impact on the remaining three aspects. Current immobilisers are reasonable value and a smart card system might improve their security because it would be a two-factor system requiring something the driver knows, as well as something he carries (or is). The state diagram that follows shows the different security states that could be achieved with the system envisaged.

STATE DIAGRAM
Vehicle security states


OPEN
Doors unlocked
Theft alarm activated
Seats and mirrors adjusted
Card inserted in contact reader. Authentication code matched
(PIN, biometric or other) or
[Valet code keyed in]
Arming code sent to ignition and fuel systems.
Release code sent to brakes, steering and bonnet catch.
(Locking release pressure reservoir pressurised opened)
Doors lockable / unlockable manually.
READY
Ignition and fuel systems armed but off
Doors as manually selected
Brakes, steering and bonnet catch released to manual operation
Card in proximity to contactless reader
(Release code supplied to doors)
Card removed from proximity of reader when valet code not set
Ignition and fuel systems disarmed.
Locking release pressure reservoir depressurised. (Battery operated pump)
If no weight on any seat for 'X' seconds and all doors and windows closed then doors, brakes, steering and bonnet all locked. Theft alarm sensitised.
Switched off
Normal vehicle controls
LOCKED
Ignition and fuel systems disarmed.
Doors, brakes, steering and bonnet catch locked.
Theft alarm sensitised
RUNNING
Ignition and fuel systems on.
All systems operate as normal.

Notes

1. If valet code keyed in the vehicle may only alternate between ready and running. The owner may remove the card

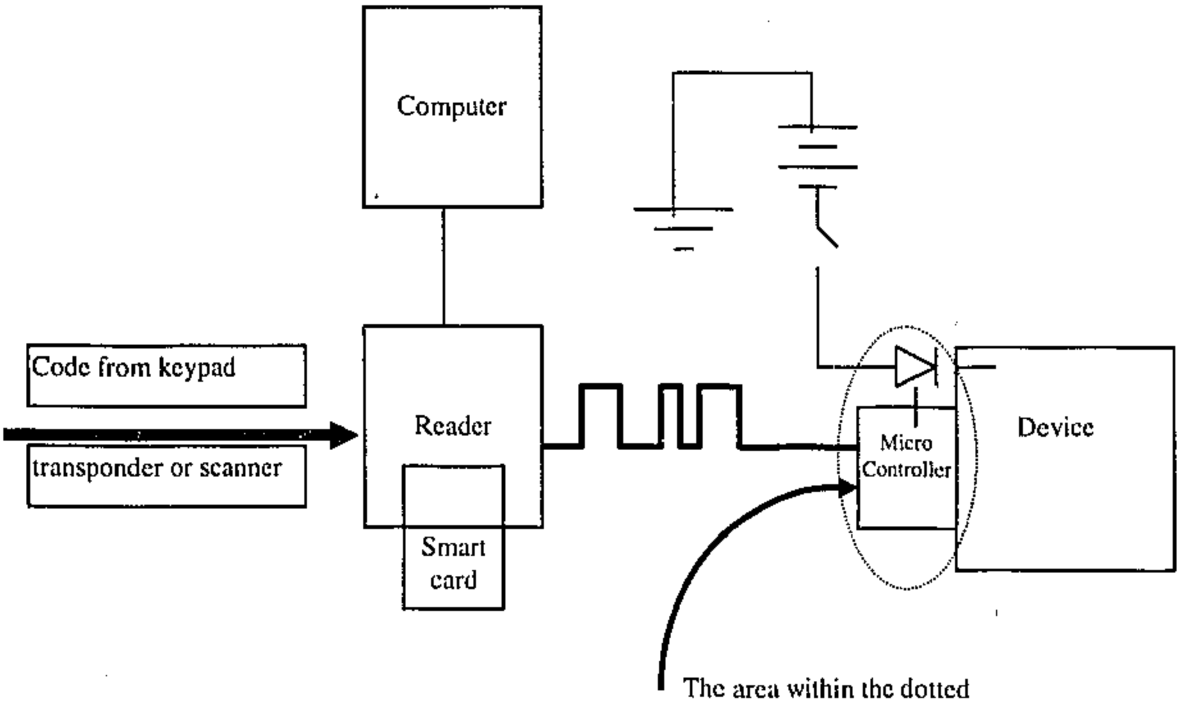
2. A dual chip card is assumed to be in use

Figure 13

The system might be a little more convenient, since if the smart card was removed the vehicle would automatically be immobilised. To demonstrate the technical simplicity of a smart card controlled vehicle security system, a hardware simulation was constructed. The block diagram of the simulation that follows demonstrates the two-factor aspect of a smart card system. The Pascal code needed to extract the activation key from the card is at Appendix 7, and the Motorola assembler code needed to compare it to the key stored in the vehicle actuating microcontrollers is at Appendix 8

THE SIMULATION

A block diagram of the main components of the system



The area within the dotted ellipse to be encased in rigid thermosetting resin so that it cannot be bypassed without damaging the device

Figure 14

The simulation was constructed using a variety of components, see Figure 15. The smart card was from Smart Silicon Systems Ltd (SSS) and incorporated a Hitachi H8/310 chip supporting their smart card operating system (SCOS). Since only a basic reader was available, enrolment was carried out using the SSS Merewin program that loads on a PC and enables the reader to be manipulated. The PC was required because the available card was application specific and not programmable by the researcher. For a more realistic simulation a programmable card, such as the Java cards, Smart Card for Windows or GemXpresso would be needed together a reader with an integral keypad, as these are now available at a reasonable price. Alternatively, in the unlikely event that access was granted under contract by Mondex International, a program could be written for a Mondex card in MEL. During enrolment a codeword was stored on the card, but in a more sophisticated system, a biometric template would have been used. Using a standard terminal emulator package, ProComm, the same codeword was stored on a microcontroller that was representative of the microcontrollers found on a modern car. The particular microcontroller is a Motorola MC68HC11 that is commonly used as an engine controller. Using a Motorola development board the small assembler program at Appendix 8 was also stored on the HC11. Finally, the Pascal program in Appendix 7, running on a PC, enabled a user to direct the smart card to pass the codeword to the microcontroller where the assembler program compared it to the previously stored codeword and, if the two matched, sent a group of pulses to the thyristor between the power supply and the device. If the thyristor did not first receive the pulses, power could not reach the device. Security, therefore, depended upon the user having been enrolled, being in possession of the smart card, and knowing the codeword to activate the Pascal program. Additionally, it depended upon the microcontroller and thyristor being mounted on the device in such a way that they could be neither removed nor bypassed without incapacitating the device. With potting resin this would be possible.

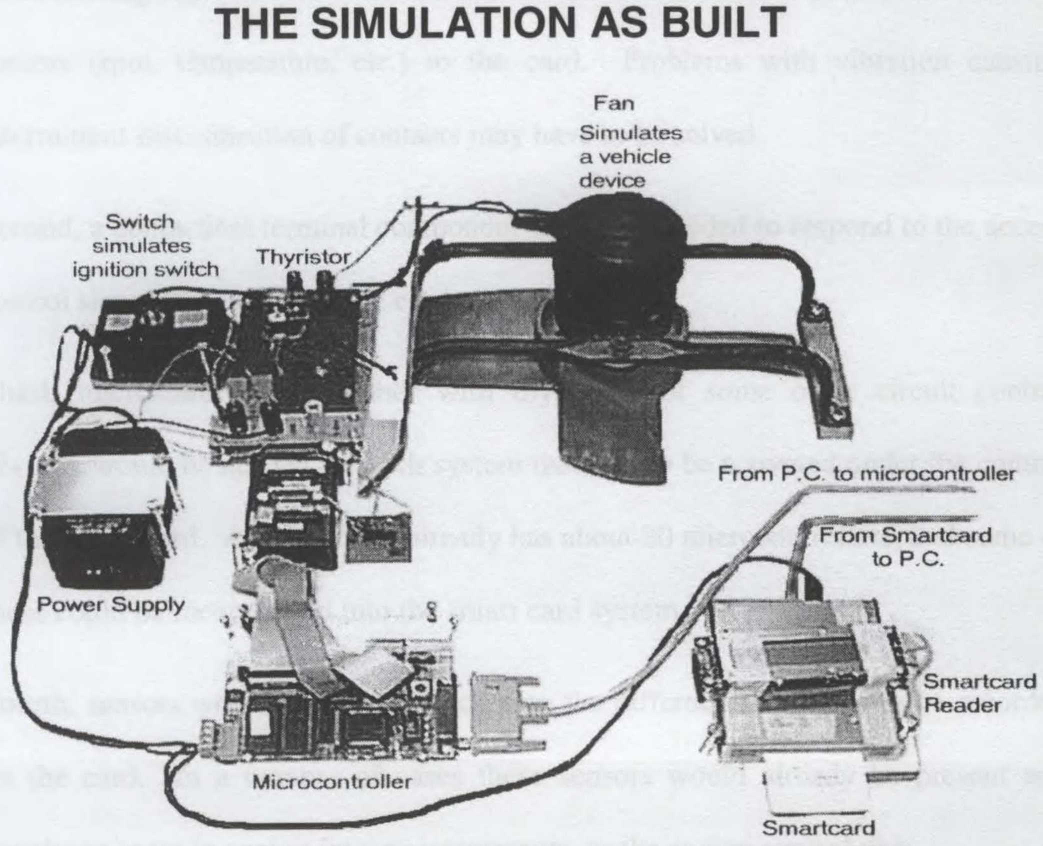


Figure 15

The simulation demonstrated only the security aspects of vehicle management and, in particular, no attempt was made to assess the response time of the card used. In a more ambitious simulation a combi card, as described in section 2.7.6 could be used, if a programmable version could be found, and the feasibility of contact with external authorities examined. For the limited demonstration to be expanded into a smart card management system installed on a vehicle, a number of vehicle modifications would be necessary and some devices would need to be installed, as follows.

- First is a smart card access module (SAM). A contact reader component of this module would be required to obtain the activation key and any data required for personalising the vehicle. The SAM should be able to write data obtained from sensors (rpm, temperature, etc.) to the card. Problems with vibration causing intermittent disconnection of contacts may have to be solved.

- Second, a contactless terminal component would be needed to respond to the access control signal if a dual interface card was used.

- Third, microcontrollers, together with thyristors, or some other circuit control devices, would be needed for each system that was to be activated under the control of the smart card. A modern car already has about 20 microcontrollers, and some of these could be incorporated into the smart card system.

- Fourth, sensors would be needed to capture the different data items to be recorded on the card. In a number of cases these sensors would already be present and supplying input in analog form to instruments, or the engine control unit.

- Fifth, an input device might be needed to enable the driver to interact with the card. This could be a keypad to accept a PIN and/or codes covering usage. If a biometric feature was to be used to identify the driver then an appropriate scanner would be needed.

- Sixth, if the application called for the contactless payment of tolls or parking charges then some form of transmitter would have to be installed.

- Finally, an output/display device could possibly be required if the application envisaged external authorities, or others, communicating with the driver. Conceivably the output could be by voice using some form of wireless transmission.

This list presumes that current automotive technology has continued in use. In the event of futuristic developments such as "drive by wire" control, or a manufacturing and distribution process driven by e-commerce technology, other presently unforeseeable modifications might be necessary. Whether or not these developments occur the modifications would add to the cost.

6.5 Security cost and Perceived Benefit

6.5.1 Perceived need for security.

Potential security benefits must be related to their need as perceived by owners and their cost. There is no unanimity as to the needed level of security. Geason quoted UK Home Office Consultants on this point. In 1985 the Consultants believed that better vehicle design could contribute to security and indicated that necessary security features should include:

- better locks for doors, steering, and ignition, laminated window glass, protected bonnet and boot catches and audible reminders of carelessness, such as leaving doors unlocked.

These features might cost more than many owners would pay, but the Consultants then mentioned:

- alarms,

- central locking, and
- engine immobilisation.

6.5.2 Cost of smart card facilitated vehicle security

When considering card system security, as with all security, the need must be balanced against the cost and, according to Geason, the Consultants estimated that car buyers might pay up to US$100 extra for effective security. However, she also quoted manufacturers as saying "security doesn't sell cars"(Geason & Wilson, 1990). Since fewer than 10% of claims against vehicle insurers relate to vehicle theft, it is unlikely that any reduction in premiums will be enough to pay for the cost of adequate security. A general conclusion is that, if smart card supported security systems are to be part of vehicle design, the systems should be incidental to other features for which the buyers will be prepared to pay. What Australian motorists might be prepared to pay is now examined. If a smart card security system could be provided at close to the same cost as an immobiliser, then it would probably be chosen because of the extra facilities it would provide. Since individual owners seemed to be satisfied with present usage and maintenance control arrangements, it may be assumed that they would not be prepared to pay much to improve those aspects of any management system. Security is probably their main concern, and therefore, in an effort to determine how strong was that concern, a questionnaire was distributed to 300 vehicle drivers in the Edith Cowan University , Mount Lawley car park and eighty five responses were obtained. The questionnaire is at Appendix 9, and a table summarising the responses follows. The results, necessarily limited and possibly not truly random, nevertheless suggest that owner-drivers would like better security, but would be prepared to pay only from A$100 to A$500 for it.

Table 6: What motorists might pay for security

CAR PARK OPINION SURVEY

QUESTION	NUMBER AND PERCENT GIVING INDICATED RESPONSE									
	More	$500	$100	$50	$25	$10	Less	Yes	No	Total
What would you pay for ultimate security?	1 1.2%	26 30%	32 38.5%	8 8.4%	4 4.5%	12 14.5%	2 2.4%			85 100%
What would you pay for pretty good security?	-	8 9.6%	31 34.9%	23 27.7%	5 6%	11 13.3%	7 8.4%			85 100%
Is standard security enough?								30 36%	55 64%	85 100%
Are alarms/immobilisers worth fitting?								71 84%	14 16%	85 100%
What would you pay for an alarm/immobiliser?	-	7 8.4%	40 47%	17 20.5%	3 3.6%	4 4.8%	14 15.7%			85 100%

All figures in A$

Fleet managers accepted that the present security arrangements already cost something, and for a better system, would be prepared to pay a little more. None was prepared to give an opinion as to a specific figure without detail about what a smart card system might do: however, in conversation, for a total system providing both security and management, one percent of vehicle cost was mentioned. This would be about A$200 per vehicle.

6.6 Summary

As a result of these investigations it has been determined that a smart card suitable for use in vehicle management would probably need a dual interface should have between 20K and 30K of rewritable memory. A dual interface chip might meet the technical requirement for access and activation, but might not gain widespread use for reasons unrelated to vehicle management (e.g., financial institution misgivings about security). Vehicle fleet owners might be interested in a smart card supported management system if it was cheaper than existing vehicle logging devices, but the upper limit of one percent of vehicle value is possibly based more on optimism that any firm limitation. Apart from very elaborate security involving biometric identification, only ten percent of owner-drivers indicated they were prepared to pay more than one hundred dollars. For a full system, vehicles would require quite extensive and expensive modifications.

7 RESULTS & PREDICTIONS

7.1 General

The first chapter poses four questions.

- What technical advances are needed and what might be expected?

  Technology generally is considered in chapter two, and some aspects specific to vehicle management, in chapter six. Now, required improvements and technical expectations are described in sections 7.2 and 7.3.

- What problems might impede improved personal mobility?

  Problems, as it turns out mainly of a non-technical and non-commercial kind, are discussed in chapter four. In sections 7.4 and 7.5, this chapter considers what solutions might be feasible and whether regulatory action might facilitate them.

- What commercial developments and changing public attitudes might result in an environment conducive to a smart card supported system.

  This question resolves, after discussion in chapter five, into an evaluation of the possibility of a "killer application". The prospects of each of the candidate "killer applications" are evaluated in section 7.6, and, as an alternative, a projection of possible growth, based upon published actual figures and industry forecasts, is presented in section 7.7.

- What is the perception of the need for improved personal mobility, including better vehicle management?

  Chapter three outlines the possibilities for better management but perception may not be the same as reality, and this aspect is examined in section 7.8 before drawing a general conclusion.

7.2 Required improvements

7.2.1 Chip architecture

When considering the advances needed to make smart cards practicable and acceptable for a wide range of applications, it must be borne in mind that events may be influenced by apparently unrelated developments such as faster higher-capacity communications disintermediating the motor industry, the development of alternatives to liquid fossil fuels, "drive by wire designs", a heightened public concern about pollution, and any number of other currently unforseen possibilities. However, disregarding such unpredictable events, it is still clear that improvements are required to the cards themselves, both hardware and software; to peripherals and infrastructure; and, to associated technologies such as biometric identification. From this limited perspective the outline of an ideal multi-application architecture might be like that illustrated in the block diagram at Figure 16.

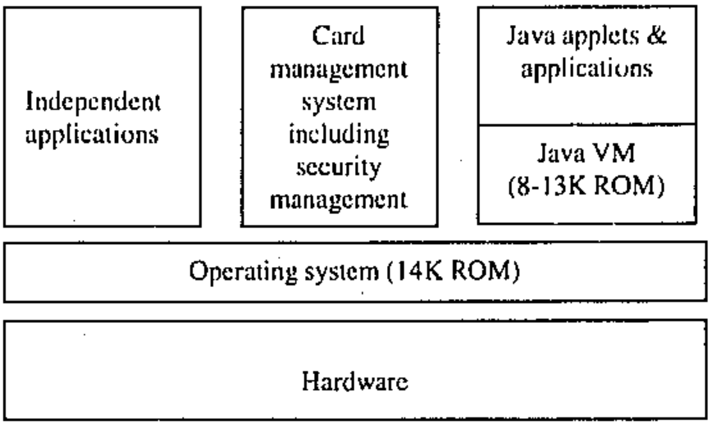

Independent applications
Card management system including security management
Java applets & applications
Java VM (8-13K ROM)
Operating system (14K ROM)
Hardware

Figure 16: An idealised smart card architecture.

The card management system may be considered analogous to a data base management system and it will be needed to control the loading and unloading of applications, and to maintain their security, integrity, and independence. Block labels indicate the functions of other components in this scheme. This architecture would be needed to support the multi-application card that has been assumed to be necessary to promote ubiquitous smart card use.

7.2.2 Chip improvements

As estimated in chapter six, existing normal smart cards, even those with 16-bit processors and 16K of EEPROM, are inadequate to provide all, or even most, of the desired applications. A more powerful card is needed. In a multi-application card for general use, the chip will need a cryptographic facility which will probably be asymmetric. For reassurance, the key is likely to be at least 1024 bit, and much of the work of encryption will be carried out in a hard-wired co-processor. For security, at least parts of the facility should be in ROM; and, for speed, access will require more RAM than is now normal in card chips. If the chip is to compare biometric features, then it will need even more processing power. To produce acceptable results, it will need to have increased reliability, faster enrolment capability, and improved discrimination between biometric features. It will be recalled that in chapter six the requirement for non-volatile, rewritable memory for a comprehensive vehicle management system alone was estimated as 18K. As mentioned in section 2.7.4, chips with 32-bit words and 32K of rewritable non-volatile memory capable of being installed in smart cards have been designed, and at least two, the CASCADE chip and Motorola's M-Smart Jupiter, even manufactured. No applications are known to have followed, probably because the resultant smart cards so far have been considered to be too expensive by potential issuers. Both the CASCADE and the Jupiter chips need 32-bit processors because their code is interpreted rather than native (P. Spalding, Senior Engineer, ERG, personal communication, July 11, 2000). Given a large enough demand it is probable that the requirement could be met. Overall, bearing in mind that the potential for card improvement is heavily weighted by that for chip improvement, what emerges is a requirement as follows:

Table 7: Required and available chip features.

Feature	Probably Required	Now available
EEPROM	32K	16K
RAM	1K	256 to 640 bit
ROM	30K	25K
Clock speed	20 MHz	3 to 14MHz
Word size	16 bit	8 or 16 bit
Circuit density	0.35 micron	0.7 micron
Power	1.8 V	3 to 5 v
Current	< 1 to 10 mA	< 200 mA

Note: The parameter values shown under "now available" are not all available on any one card chip.

This hardware requirement could be as illustrated diagrammatically in Figure 17.

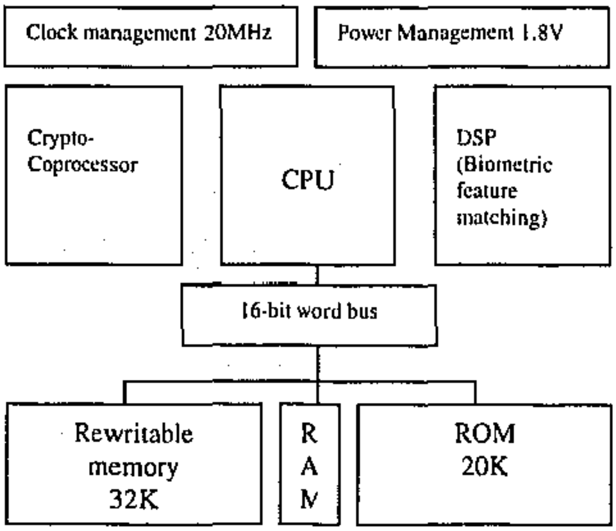


Figure 17: Required chip features.

7.2.3 Card manufacture and chip embedding

Reductions in card costs, as distinct from chip costs, would be helpful and this might be achieved partly by obtaining economies of scale, as discussed in section 7.4, and partly by more efficient manufacturing technology. The main task in manufacture is to embed the chip in the card: a far from a simple process. There are two technologies.

- With PVC laminated cards, the core lamina is printed and has a recess milled in it, the chips are formed with contact plates into modules that are attached to an epoxy bonding tape. The tape, which bonds on one side to the plastic and on the other to the chip silicon, is chopped into units that are pressed into the milled recesses, a coating of resin is applied and then ground flush, and outer transparent laminae are added. The work is almost completely automated and, although even in 1992 an output rate of 1800 cards per hour had been achieved (Baker, 1992), further improvements may be possible.
- With ABS cards the process is different. The chip and contact plate module is placed between outer laminae, and the core lamina is injected to fill the space and surround the module (Benhammou, 1997). At least for small runs the basic process is cheaper, but the cards are more difficult to print.

In either process, some manufacturers embed the module in a lead frame to protect it from stresses imposed by flexure of the card: no doubt, this adds to the cost. What is needed is a satisfactory method of printing on ABS, together with a cheaper system for manufacturing large batches.

7.2.4 Biometric identification

Biometrics technology needs improvement in three areas.

- The most obviously useful development would be a biometric identification method that met the financial institutions' required FRR of 1 in 100,000.
- A second requirement is a smaller cheaper scanner.
- Finally, there is a need for a reliable standardised testing methodology that will enable specifications to be written so that vendors' claims may be compared independently and objectively. In this respect the International Computer Security Association (ICSA) certification, and similar efforts, should be regarded merely as an interim step.

7.2.5 Vehicle management

Potential improvements in vehicle management have been given in chapter three, and the necessary consequential modifications for their implementation in chapter six. If consideration is limited to improved security, keys that incorporate transponders, without which the vehicle will not start, are now commonplace; but, two-factor security should be developed and it should employ biometric identification.

To summarise, the technology improvements needed are:

- more powerful, cheaper smart cards, structured to support multiple applications,
- either more discriminating biometric identification technology, or a more relaxed FRR requirement,
- cheaper smaller scanners,
- more reliable, standardised biometric identification device testing, and
- kits to implement inexpensively the modifications listed in chapter six.

7.3 Technical expectations

7.3.1 General

Assuming the requirements have been identified, the question of if, and when, they might be met, must be addressed. Although not yet adequate to support multiple applications, smart cards will certainly improve in size, circuit density, power required and memory over the next few years.

7.3.2 Circuit density and size

Circuit density increases and size reductions would seem to be inevitable in both the research and manufacturing environments. For example:

- Chicago University has announced that it can make chips with tiny features using a process called SCALPEL; a process that uses electrons rather than photons to define the etching of chip circuitry. Densities of the order of 0.076 microns are claimed ("Cutting chips", 1997).
- Intel has announced that it now has a technique that enables it to store twice as much memory on the same area of a chip, and IBM has said it had found a way to replace aluminium conductors in a chip with faster, cheaper copper ("Chips ahoy", 1997).

These advances might eventually be exploited in smart card chips, but even without such spectacular advances, chip density has been increasing. For example, three years ago the circuit density of CMOS transistor chips, including EEPROM technology, were at the 1.8 micron level; whereas today's state of the art is 0.6 microns, which is expected to fall to 0.35 microns by the year 2000 (Benhammou, 1997).

7.3.3 Power supply

Contact cards have chips that normally require 5V supply, whilst SIM cards conforming to the GSM 11.11 standard, function with only 3V; but the variation in power supply is probably more a matter of conformance to standards than a technical necessity, and today, card chips requiring only 1.8V are manufacturable.

7.3.4 Memory

Memory, especially non-volatile memory, is a different matter. As Henry Mundt, executive VP, global deposit access for MasterCard International, and Mondex CEO, Michael Keegan, said in a joint interview with Electronic News, in 1997,

> "MULTOS is 'the Windows for smart cards' and current-generation smart card microcontrollers (MCUs) will be capable of supporting MULTOS, but the true benefits will come when chip makers can get more memory around their logic for smart cards, which they expect will occur in 1998. When the ICs can offer 16 kilobytes EEPROM and between 28 and 32K ROM in the tight 25 square millimetres of silicon on the cards, the multi-application card will be a reality," Mr. Keegan said. "Such ICs will be freely available in the '98 time frame," he predicted. "The MULTOS platform is viable now," he said. "It's just not as capable. Listen, a PC was still a practical product when we were running new applications with the PC's 120K of memory. The real story is that we're now looking at a programmable smart card (with MULTOS), and that has not happened before. Every solution had to be hard-wired by the silicon maker." ("Smart cards in spotlight", 1997, p. 8).

Allowing for marketing optimism, and bearing in mind that MULTOS is only one option for the industry, it seems likely that the technology Mr Keegan described would be available as soon as there was a commercial requirement for it. Today, in the year 2000, only the CASCADE card and MIFARE.PRO with the SmartXA chip come close to providing the features he named, and it should be noted that for vehicle management the card might need even more EEPROM than he envisaged. Keegan made no mention of cost. The major non-commercial Mondex smart cards pilot scheme completed so far is that by the Exeter University, whose Joint Technology Applications Project (JTAP) report in late 1999, concluded among other things that:

> "...smart cards are moving towards support for multiple applications on the card, but this is severely limited by the memory capacity of present cards." (Cannon & Wooderson, 1999, p. 3).

It would seem that as yet there is insufficient demand for large memory chips.

There is also a potentially improved rewritable memory technology, called magnetoelectronics. New magnetoelectronic devices, based on the integration of magnetic and semiconductor materials, can be used for developing smart magnetic sensors, magnetic media reads and MagRAMs (magnetic RAM memory). Initial statements say that the technology may produce memory devices that are cheaper, require less power, be faster to read and write, and be as enduring as any of the current non-volatile memory technologies (Wayt Gibbs, 1999).

7.3.5 Contactless requirements

For the contactless card the requirement is for speed rather than memory and the expectations are more optimistic. According to Roy DaSilva, NEC Electronics' product marketing manager, NEC's capability in ferroelectric RAM (FeRAM) will help the company gain entrance to the smart card market. He said:

> "We are entering this market backed by the fact that we have already made significant investments in ferroelectric RAM, which gives the speed of RAM with the programmability of EEPROM and permanent storage of ROM in a single device." ("Smart cards in spotlight", 1997, p. 8).

Again, the optimism should be regarded with caution. FerroRAM has a serious weakness in that each "read" must be accompanied by a refresh operation that restores the memory state. The process takes only about 100nS but a power failure during that time could corrupt memory. Nevertheless, judging by the New Scientist article quoted in chapter two (Fox, 1995), the required performance might be achieved. Furthermore, the JTAP project team, reporting on the use of the Mondex purse by the Exeter University, believes that FeRAM will become the preferred memory for all smart cards in the near future (Cannon & Wooderson, 1999, p. 18).

7.3.6 Biometric identification

Current performance rates are FAR, negligible, and FRR, 1:1000. These rates are well short of the financial institutions requirement of FAR, 1:20 and FRR, 1:100,000. There seems little likelihood of any biometric method meeting the FRR required by the financial institutions within the next few years. Not only does such a development seem unlikely, but one must question the need for such a high standard. Possibly, the problem might be ameliorated by the use of variable thresholding in which the laxity of the threshold is automatically adjusted to match the importance of the transaction, or commercial pressures may force the financial institutions to accept a lower FRR. Biometric identification, despite the FRR problem, will probably improve.

- Smaller, better scanners will almost certainly be developed, and, if the market expands, costs may fall. For example, Veridicom is promoting a capacitive sensing fingerprint scanner that is claimed to be no bigger than 2.5cm square and cheaper than current optical types, and Identix has countered by claiming that it will soon have developed an optical scanner no bigger than a 25mm cube - but neither firm has released any performance figures.
- Better performance and testing, faster enrolment and verification and reduced invasiveness will almost certainly be achieved, although the difficulty of truly objective testing of biometric methods has still not been solved. Sandia Laboratories undertook an assessment of biometric methods in 1991 and this is believed to have been updated in 1995, but an inquiry about the outcome drew the response that the

results were not being released. Therefore, it is difficult to be hopeful about any early breakthrough, but nevertheless, under the auspices of the Biometric Consortium, research into testing methods is continuing, and presumably, in time, methods will be developed that will enable the independent, repeatable testing of products. In the UK, a workgroup of the Association for Biometrics (AfB) has developed a statement outlining its view of best practices in testing biometric devices, but, as yet, there are no reports defining any specific method of testing, let alone results from actual tests.

7.3.7 Summary

In the light of the requirements and expectations described in this and the preceding two paragraphs, and despite the accompanying caveats and shortcomings, informed opinion appears to confirm the conclusion reached in chapter two that today's technology could produce a functioning, if not fully satisfactory, smart card supported vehicle management system. With the possible exception of biometric identification the obstacles to a better system appear to be non-technical, and the technology will be found to be adequate when and if the demand emerges. These non-technological obstacles are now examined.

7.4 Possible progress in overcoming non-technical difficulties

7.4.1 Standardisation

Section 4.3 describes the lack of standardisation as one of the major obstacles to the widespread use of smart cards. Progress in defining and conforming to standards has been slow because regulatory authorities believe that conformity should not be imposed, since attempts to do so might stifle innovation. However, a degree of standardisation is inevitable once the technology stabilises and the pace of innovation slows. What usually happens is that, initially, each contender seeks to become the dominant player, and force all the others into niches or supporting roles, but as soon as any one contender seems likely to be successful the others unite. At this point a single standard or dual competing standards may be agreed, and regulatory assistance might be useful. At present, in smart card technology, there is little to be done except await the outcome of the ongoing struggle for competitive edge.

7.4.2 Cost reduction

Cost trends for the past ten years are discussed in section 4.4. The improvement needed, which is partly technical, is a reduction in cost, but this is unlikely to happen until design is stabilised and a mass market created, because cost reductions may not be achieved until economies of scale justify more investment in automating the process. More recent reports show no evidence of any cost fall. Late in 1999, Exeter University reported its Mondex system cost per issued smart card as being £15 plus £20 for programming and personalising, which is expensive compared to (admittedly limited) magnetic stripe solutions; and, Edinburgh University cancelled its Mondex project, citing cost as the reason (Canon & Wooderson, 1999). Christophe Dolique, formerly of Oberthur, is quoted in the January 2000, online issue of Card Technology Today, as estimating that in 1999 smart card chips cost an average of US$1.33. If true, this estimate does indicate a fall in cost ("Juiced up chips", 2000), but should be weighed against the evidence to the contrary presented in section 4.4 and here. A FaulknerGray report by Don Babalon quotes Andrew Phillips, a UK-based analyst for the Dataquest unit of the Gartner Group, as giving the average price of microprocessor cards as:

1998	US$3.05
1999	US$3.79.

(Babalon, 2000). Apparently the desired reduction has yet to be achieved.

7.4.3 Improved chip and transition to it

The specification for a chip to provide the required improvements in performance seem close to being met by the specification for the CASCADE chip, reportedly to be produced by Texas Instruments for Gemplus in 1998. However, Motorola (its card chip manufacturing now by Atmel), Hitachi, Siemens (now Infineon) and SGS-Thompson (now STMicroelectronics) are all producing card chips of the current type and have not announced any intention to produce anything to compare with CASCADE. Motorola has announced an M-Smart series that includes a "Jupiter" chip, that is 32-bit and uses RISC technology, but gives no detail of its rewritable memory size. In addition to the requirement for an improved chip, there will be a need to cope with a difficult transition and so, for at least an interim period, smart cards may need to be dual-chip (contact and contactless) and hybrid (retaining a magnetic stripe).

7.4.4 FRR reduction

As mentioned earlier a biometric method that met the false rejection rate (FRR) of the financial institutions is highly desirable, but the actual standard specified (1:100,000) must be questioned. The institutions are said to claim that the very high standard is required because they cannot afford to offend genuine customers, but with the current system it is not unusual for an ATM to malfunction and fail to perform as requested. The institutions seem able to absorb any resentment that ensues. Problems with the rejection of authorised persons could be solved by offering alternative methods (Fak, 1991). Eventually, failing a device that meets the requirement, public demand may force its relaxation.

7.4.5 Biometric ID method industry certification

Until the time that a reliable biometric testing method is developed, purchasers will have to rely on the certification processes of the ICSA, IBIA and BioAPI. The ICSA process has already resulted in six products being certified ("Standards set", 1998). Product specifications, with which vendors will be required to comply, will probably follow. Smaller scanners and faster processing methods are likely to emerge. Although the use of biometric identifiers is expanding, this has been in areas where fairly relaxed false acceptance and false rejection rates (FAR & FRR) are acceptable. Employers, welfare organisations and exhibitors, amongst others have required clients to identify themselves by providing a biometric feature for scrutiny. These applications are effective even with very lax false acceptance and rejection rates. Examples are the Atlanta Olympic games, attendance recording in the workplace, identification of beneficiaries, and rapid processing of international travel approval at airports. It seems likely that for the next few years, acceptance of biometric identity verification using smart cards will occur only where lax false rejection rates are acceptable and the people to be identified are relatively powerless. General acceptance may not occur until the banking requirement is lowered or met. No evidence of any such development has been discovered.

7.4.6 Contactless card costs

The main apparent market for the contactless card is in public transport ticketing. People who normally travel by public transport are unlikely to be wealthy, but because of the extra circuitry, contactless cards are more expensive than contact versions and, in view of the nature of the target market, this expense may discourage their widespread use. In section 2.7 the potential for better rewritable memory with ferroRAM is mentioned, but the source gives no indication of the likely cost of the new technology (Johnstone, 1998, p. 38). The flaw in ferroRAM mentioned in section 7.3 is not as serious a drawback for ticketing as it might be in a financial application, such as the electronic purse or e-commerce, because readers could be designed to reject corrupted tickets and the consequences could be handled in the same way as those for defective tickets rejected by a multi-rider.

7.4.7 Vehicle Security and cost

Immobilisers are now factory fitted to Australian assembled cars, and this class of vehicle is probably safe from theft by impulse thieves so long as the driver takes reasonable care. However, Victorian experience shows that they are not immune to the attentions of professionals ("Thieves beat car giants", 1996). Cheaper vehicles are still easily stolen and even middle to upper range cars, as they become older, will become vulnerable to the less organised thieves, partly because their mysteries will become known to the thieves and partly because many owners will fail to maintain the anti-theft devices in as-new condition. Despite advances in technology, economics will dictate the level of protection and, without either incentives or compulsion, owners will probably merely continue to rely on insurance to indemnify themselves against loss.

7.4.8 Summary

With the exception of the lack of standardisation and problems with biometric identification, most non-technical problems relate to cost and their solution will probably depend on the achievement of improved cost-effectiveness.

7.5 Regulatory expectations

7.5.1 Traffic regulation enforcement

Although traffic regulations vary from one country to another WA is fairly typical and will be used as the main example. When of interest the special situations in other countries and states will be mentioned. Are changes in traffic management to be expected in WA or elsewhere? There are repeated calls for improvements in traffic management to achieve reductions in accidents, road congestion, pollution and the cost of road construction and maintenance, but there is some hypocrisy. Accidents could be reduced if speeds were reduced, and extra automatic speed traps might achieve this object, but extra traps would cost more money whereas, if they achieved their object, fewer fines would be collected. Road congestion could be avoided if more commuters used public transport, but it is hard to separate a motorist from his car, since each wants someone else to use the public transport. Exhaust pollution is easy to detect and could be reduced by normal enforcement methods, but moves to do so have proved unpopular. Taxes on fuel, and vehicle registration fees, after meeting the cost of road construction and maintenance, are a net contributor to public revenues. ("Facts", 1997). In short, although there are occasional calls for action (such as road pricing and stricter enforcement), remedies using smart cards or not are unlikely to be implemented in the present climate of opinion. Discussion with Main Roads WA indicated that it is regarded as politically hazardous to strain the link between a man and his motor car and, therefore, changes will probably rely on education and other non-coercive influences upon behaviour.

7.5.2 Road pricing and parking fees

The use of smart cards in vehicle management would be given considerable impetus if traffic authorities created more turnpike roads, or congestion controlled areas, and parking authorities established parking zones that accepted payment via smart cards. All three of these possibilities are under investigation worldwide.

- In Singapore (see section 3.2.4) a full system that uses contact cards has been installed. The contact cards are inserted into in-vehicle units that transmit and receive signals to and from overhead gantries to achieve the contactless access function. The card is a stored value card that can be used, not only to pay tolls but also for other cash transactions in supermarkets and petrol stations.
- In Melbourne, Victoria, in a venture called OneLink, the Perth company ERG had problems with finalising its automatic fare collection scheme, and was able to complete only with the support of the international giant Motorola ("Motorola-backed ERG", 1997). The project, after overcoming these problems, now appears to be functioning satisfactorily.
- In Sydney, an electronic system for collecting harbour bridge toll fees uses a stored value rechargeable smart card, and there is a toll system for the Sydney Eastern Districts tunnel.

Nevertheless, there seems little chance of specific action in WA.

- A proposal to build a turnpike road from Karratha to Shark Bay has disappeared without trace ("Toll road planned", 1996).
- Congestion and pollution control by charging vehicles for entry to specified zones has not been given any public airing.

- An "issues and directions" document distributed by Main Roads WA, gave traffic congestion as a key issue, and then, under "current directions", listed nine remedial actions, but not road pricing.
- Under the heading "future directions", the tentative option, "Look at discouraging unnecessary road use through possible road use charging", was twelfth in a list of 14 possibilities ("Issues", 1996).
- City and Local Authorities, when contacted by telephone, said their organisations might move to a smart card supported parking system if this becomes the norm elsewhere.

In short, if the authorities are moving towards a user and polluter pays policy, the movement is slow.

7.5.3 Minor control improvements

A study of policy papers issued by Main Roads, WA, seems to indicate that traffic management will be a matter of minor traffic control improvements, such as improved intersection control, data collection, and education. Officials are at pains to assure the inquiring public that any surveillance is only to monitor traffic patterns and densities and that there is no capability to identify vehicles, nor is it policy to seek it. The official perception is that higher authorities fear that the public will be hostile to any system with a potential to support surveillance.

7.5.4 Summary of traffic regulation prospects

Apparently congestion and pollution are to be controlled by informing and educating the driving public, and there is no proclaimed intention to change the present traditional methods of monitoring driving behaviour. A number of statements in the discussion papers do indicate a government wish to encourage the use of public transport and, no doubt, any smart card application that improved its convenience would be welcome, but no regulatory action to compel the application of the available technology is foreshadowed. Apparently, regulatory authorities intend to follow, rather than lead, and the use of smart cards will gain no direct support from them.

7.5.5 General Government applications

Even if there is little expectation of regulatory action directly relating to roads and vehicles, there is the possibility that some general government strategy may lead to the widespread use of smart cards. According to a report in the daily newspaper The Australian, the Federal Government, in January 1998, announced that it would begin to buy application space on about 2.7 million private smart and credit cards in 1999 ("Government agencies", 1998). This was a rather surprising statement as the multi-application card is, as yet, hardly a reality. The number, 2.7 million, seems to suggest that the Government had the Telstra card in mind. In September 1998, as mentioned in section 5.9.4, a number of leading smart card companies wrote to all Federal ministers, warning that the country risked being left behind because of Government inaction ("Smart card makers appeal to Canberra", 1998). However, it could be that the Government had become aware of the difficulties of what was proposed. In the UK, the Federation of the Electronics Industry (FEI), in 1996, pressed the Government to establish a multi-application smart card for all government employees, that would fulfil key requirements of Government, and be a stimulus to, and basis for, commercial applications. Two years later a follow-up showed that no progress had been made ("Role of Government", 1998) and, even now, there are no reports of any action. The situation in the US and Canada has followed much the same pattern. It seems that the implementation of smart card systems is unlikely to be driven by regulatory action.

7.6 Commercial expectations - non-vehicle

7.6.1 Introduction

Failing either solutions to the non-technical problems or regulatory action, the next question is whether normal entrepreneurial processes will cause some "killer application" to emerge to form the core of a multi-application card of which one application might be vehicle management. Candidate applications are examined in this section, commencing with those in finance. The three financial possibilities introduced in section 5.3: namely, a cash payment substitutes system, including an electronic purse, e-commerce and e-shopping are now evaluated as possibilities.

7.6.2 The purse and banks versus merchants

Financial institutions (see section 5.3.2) are accepting smart card technology only slowly. In the USA the investment in the excellent existing infrastructure, the handsome profits made from online credit and debit authorisations, and the fear of a systemic breach, will probably ensure that financial institutions are followers rather than leaders in any move to make wider use of smart cards. Credit and debit cards may be upgraded by using smart cards instead of magnetic stripe devices, but there appears to be no move by the institutions to promote a multi-application capability. The trial of an electronic purse system in Manhattan by four major US financial organisations has been reported as a failure, as has a trial in Guelph by the Canadian Mondex banks. In Manhattan, Citibank with VisaCash combined with Chase Manhattan and Mondex in a joint pilot scheme. Six hundred merchants, who were not required to pay for the readers, are said to have been frustrated by early technical faults and, although about 95,000 cards were issued to residents, only 53,000 loads to the cards were recorded - an indication that many cards may not have been used at all (Foderaro, 1998). In Europe there are unresolved conflicts over who will pay, and how much, and some financial institutions are trying to force merchants to pay what the merchants regard as excessive fees for participation: for example,

> "All present electronic-purse pilots have proved unsuccessful because they have not had enough merchant support."

says Societe Nationale des Chemins de Fer Francais (SNCF) treasurer Eugene Caffart and, again,

> "We provide a critical mass of users, and we expect the users to pressure shops to accept the cards later." (Amdur, 1997, p. 4-5).

Merchants may see the electronic purse as a device that will enable the banks to participate more profitably in the cash transaction market and may regard it as a bank solution to a bank problem for which they should not be expected to pay. In Australia the four major banks (National Bank, Westpac, ANZ, and the Commonwealth Bank) announced in November 1997 that they intended to run a major trial and issue eight million Mondex cards starting in July 1998 ("Smart card invasion", 1997). Whatever their plans may have been, the banks appear to be having second thoughts, because since 1998 their activities have been confined to closed pilot schemes. Exacerbating the problems of digital cash systems, whether implemented with smart cards or online, is the difficulty of handling micropayments. As Ison of Commonwealth Bank put it

> "We are attempting to derive sufficient revenue from a transaction of, say, one dollar to pay for its processing infrastructure and deliver a commercial proposition to the five parties in the transaction, the cardholder, the merchant, the system operator (issuer), and the two banks involved." (Ison, 1996, p. 16).

Likewise, from an article in the June 1999 issue of Scientific American,

> "In the US at least, all the banks that once supported micropayments have taken their resources elsewhere" (Wallich, 1999, p. 1).

Surprisingly, within three months of the Scientific American article, the Aberdeen Group, an internationally respected market surveyor, stated that,

> "...the future acceptance of digital cash will challenge traditional means of exchanging value..." ("Dash to digital cash", 1999, p. 7).

Finding an issuer prepared to pay for a major issue of smart cards may be difficult, but achieving a substantial volume of transactions may be even more so. The conflicting aspirations of banks and merchants and the difficulties of handling micro-payments seem unlikely to be resolved soon. In addition to the disagreement between bankers and merchants, the financial institutions are fighting amongst themselves.

7.6.3 Payment standards

Failure to achieve either a common protocol standard for smart card payment applications or a common operating system has been covered in section 4.3. Major candidates for the protocol standard, the EMV and Mondex specifications, are still competing. The struggle over what operating system or application interface to use continues, with MasterCard, and Mondex, seeking to establish MULTOS, Visa, with a rival industry grouping, pressing for the Java API and Microsoft making a late but powerful push on behalf of its

Windows for Smart Cards. There is no indication that a compromise is near in any of these areas.

7.6.4 Purse battle

Behind the negotiations to achieve common standards for operating systems, interfaces and payment protocols and a fair share of profit for each stakeholder, the battle for the electronic purse market continues (see section 5.3.5) and until settled will probably frustrate efforts to establish a viable system in the US. It may be that US financial institutions will accept smart cards as debit or credit cards in an effort to reduce fraud, but probably will not pursue the idea of an electronic purse without some strong incentive to offset the attractions, and fees, of online transactions. Insufficient attention may have been given to the attitude of potential purse holders. Issuers write of the cleanliness, convenience, and improved divisibility of digital money contained in smart cards, but until the cards are able to be used as freely as money, holders may not be impressed.

7.6.5 Internet payment protocols

In addition to the purse, other potential smart card supported financial applications are cash micropayments and accrual transactions (categorised as either e-commerce or e-shopping) consummated over the Internet. There is still no agreement on Internet payment protocols. Visa and MasterCard have co-operated in developing a secure electronic transaction (SET) protocol for use in electronic payments, but although this protocol may be suitable for substantial transactions it is over-engineered for handling individual purchases or the micro-payments that are likely to be the main traffic in e-shopping ("Can current technologies", 2000). If SET was accepted for e-commerce, an increase in transactions supported by identification and encryption using smart cards would probably follow, but there are many competing systems, some involving trusted third parties and others asymmetric key encryption using software installed on PCs. In short there is no sign yet of a consensus, whilst merchants are unlikely to invest in smart card readers or join any system until it is widely accepted. Today there is talk of seeking compatibility between the PC/SC protocol and SIM cards in cellular telephones, with a view to facilitating e-commerce between mobile entities. The goal seems plausible because the SIM card already incorporates a payment capability. One may doubt the need for e-commerce on the move and note that the SIM card is a European rather than a US device, but GSM or PC/SC controlled access is one of the applications most likely to form the core of a multi-application card, since the former is already being implemented by FranceTelecom with a Cartes Bancaires card, and the latter enjoys the powerful support of Microsoft and does not depend too heavily on the acquiescence of financial institutions.

7.6.6 Public Transport Ticketing

Despite their competitive struggle the financial institutions may have no choice but to agree on a payment protocol, because transportation companies have seen the advantages of contactless cards in automating fare collection and could leverage the ticketing application by adding a purse function. In addition to the Octopus project being run in HongKong, transportation organisations are conducting trials all over the world. There are trials in South Korea, London, Paris, Rome, San Francisco and, in Australia, the Sydney Transcard scheme. All of these trials have shown promise but, with the exception of HongKong, none has been a runaway success and, again, apparently, the problem lies in merchant acceptance. Some financial institutions regard a purely contactless card as unsuitable for a financial application because a contactless application may last no more than a third of a second, too short a time in which to process a encryption algorithm. A dual-interface card may overcome this objection at some cost. Contactless cards as yet may be too expensive to be economic purely as access tokens. In this respect the Sydney Transcard scheme is particularly interesting because its contactless card, in addition to giving access to several different transportation services, includes a stored value application. Transcard has published research results showing that 56% of users were satisfied with the system, but the only information released about merchant attitudes was that 35 percent of consumers reported that the cards were not readily accepted by shopkeepers (MacSmith, 1996). However, if merchants do not support a stored value application by providing readers in substantial numbers, then users are unlikely to want it.

In WA, the only indication of a possible application is that the Department of Transport, as a feature of their "System 21" initiative, claims to be considering smart card technology as a way to improve ticketing within ten years. Although as yet, it shows no sign of doing so, public transport ticketing may become the "killer application" that the smart card industry requires, because it enjoys a defacto standard in the MIFARE specification and it has issued more smart cards than any application except telecommunication.

7.6.7 Telecommunication

The point was made in section 5.4 that the telecommunication industry has more experience with smart cards than any other sector. The following table shows the actual and forecast use of smart cards by the industry.

Table 8 Telecommunication Industry Smart Cards.

Year	Payphone cards	Mobile phone cards
1996	100m	15m
1997	220m	70m
1998	Not known	100m
1999	-	250m
2000 (est)	-	430m
2004 (est)	-	970m

(Facts and forecasts, 1999; ICMA Quick card facts, 2000).

The increase in the use of mobile phone cards and the potential for their use in an extended role has led to the belief that they could form the core of a multi-application card. Hitherto, the telecommunication companies have been prepared to sell only pre-paid cards (both pay and mobile phone), or "credit" phone cards that record the service and enable later billing. Apparently the industry did not wish to become involved in providing cards that could be used by entities outside the industry: possibly, because of the difficulties of the consequential funds clearing process. The financial institutions, for their part, are believed to be wary of any financial application using the telecommunication payments protocols. Today, in addition to information services such as news, weather and stock reports, there is discussion of providing interactive services such as banking and e-commerce including payments. For these proposed services to be implemented there will need to be co-operation between telecommunication companies and banks. Card Technology Today, an online magazine dedicated to reporting news about smart cards, writes that, in France, this proposal is already being acted upon ("France Telecom", 2000).

In Australia developments are slower. In 1997,Telstra announced that it would issue six million reusable (electronic purse) and eight million disposable (stored value) smart cards before 1 July 1998, claiming that, by contrast, Australia's four major banks planned to issue only 100,000 Mondex smart cards in the second half of 1998 ("Telstra winning", 1997). Telstra has the advantage that it is a nationwide "near monopoly" and has already issued some cards, but it remains to be seen whether it is able, or even wishes, to usurp the traditional banks' function in this way. In a pilot scheme in Adelaide, Coca-Cola and Smiths installed vending machines that would accept Telstra non-reloadable cards, but no results have been released. In Melbourne, the City council considered adapting parking meters to accept the cards, but apparently did not proceed, because there have been no further reports about the proposal ("Phone cards get smarter", 1998, January 13). In short, the cards have been used in payphones, but hardly anywhere else, since merchants appear reluctant to provide the necessary readers.

In late 1999, the ANZ, Telstra and ERG announced that they had jointly formed a transaction processing company with a centre to handle purchases. At present each of these companies uses a different purse technology, but they intend to select one, probably MULTOS, because a single standard would enable the offer of a variety of applications on a single card (Big players get smart, 1999, September 14). It would seem that, despite early optimism, telecommunication has not become the hoped for "killer application", but the potential exists and one day could be exploited.

7.6.8 Purely access applications

The majority of smart card applications may be thought of as access applications but, most of the majority, like the GSM SIM cards, involve some transfer of value. Purely access applications, such as those restricting admission to secure physical areas, networks and sources of information have been successfully implemented for some time, but none has been large scale. Such applications make no profit for the issuer, and any reduction in administrative costs is usually small.

7.6.9 Welfare benefits

In several states in the USA, smart cards, in conjunction with biometrics, have been used as the authentication device to enable beneficiaries to draw their benefits. Reports claim substantial savings and, in particular, savings that result when applicants decline to provide the biometric feature required. If beneficiaries were induced to use smart cards as identification, it would be a logical extension to provide an electronic purse on the cards, and even, perhaps, enable beneficiaries to download their benefits directly onto them. Judging by the Australian public's reaction to the Australia Card proposal, in Australia the situation is different, and the application of smart cards in welfare is likely to face great difficulties. Public rejection of identification may be expected to continue despite pressure upon the Government from industry, discussed in section 7.5.

7.6.10 Health

In Germany and France, smart cards have found a role as a store of information in health schemes, but the cards do not include a financial application and seem an unlikely core for anything except their specific function. In WA, a health insurer (HBF) announced its intention to issue 700,000 memory chip cards to its members by Christmas, presumably 1997 ("Smart card", 1997). Although it seems unlikely that a memory chip card application could be the core of a multi-application system, ERG, the card suppliers, say that whilst the current application requires only a memory chip, the chip to be used is capable of handling other applications. The intention, initially, is to use the card as an identification token, and eventually to extend it to become a multi-application system. Neither HBF nor ERG has indicated how they propose to address the problems of standardising operating systems or establishing a certification authority. These problems are discussed shortly, but, by 1999, few vendors had installed card readers that would accept payment using the cards.

7.6.11 Border control

Several pilot schemes have been introduced at airports with a view to determining whether smart cards may be used as improved passport substitutes. The first was a Dutch scheme launched in 1992, but apparently it was discontinued because a television documentary proved that it could be defeated (Overview, 1997). Other smart card supported border control schemes are still operating, but their success, or otherwise, has not been widely reported.

7.6.12 Multiple applications

The potential applications discussed in the previous paragraphs should be considered against the presumed desire of holders to have a multi-application card and the assumption in chapter one that, for general acceptance, smart cards would need to support multiple applications. The technology to create and implement multi-application cards probably already exists, as do most of the non-commercial criteria given in section 4.2 for a successful system. The problems are commercial, and the crucial obstacle is the lack of a satisfactory business case for each stakeholder. To create a suitable commercial environment requires co-operative answers to the following questions.

- Who will own the card and applications?
- Who will issue the card, own application keys and customer information and update the information?
- Who will perform application certification and authenticity?
- Who will pay for the infrastructure development?
- Who will control the advertising space on the card and its chip?
- Who will be liable for lost, stolen or faulty cards?
- Who will get the revenue streams?
- Who will own the card brand?

There are as yet no generally agreed answers to these questions and, until there are, it seems unlikely that holder expectations will be met (Barr, Allen & Burke, 1997, p66-67).

7.6.13 Holders versus issuers

Holders might desire increased functionality, fewer cards and the ability to make their own selection from amongst the applications described above, but they may then encounter resistance from issuers who want no other brands on their issued cards. As Peter Fogarty, CEO of ERG said, "It is unlikely you will have another Telco on a Telstra card." (Big players get smart, 1999). Further, if the card includes an electronic purse, the holder would want to be able to use it with a wide variety of merchants and reload it anywhere at any time. ATMs and EFTPOS terminals would need modification and further standardisation before this ideal could be achieved.

7.6.14 Operating system compatibility

Even if a killer application is discovered, it may not be possible to use it as the core of a multi-application scheme due to the struggle between the supporters of the MULTOS operating system and those of the Java API. If the financial institutions choose MULTOS and the killer application uses the Java API or some other interface, then the applications that can be built around the core might be restricted. It could be that the purse will first emerge as a method of paying beneficiaries and, if so, the banks might insist on the use of MULTOS, since they control it and they perceive it as being more secure. On the other hand the development of other uses of the card would be simplified for developers if the

Java API was employed, since it is easier to install new applications on the Java interface. In addition, non-bank participants might not trust a card with an operating system that was the property of a banking consortium, especially as the banks might reserve the right to install all applications. Although, ideally, a card should be capable of supporting Java with MULTOS as shown in Figure 16, two incompatible systems could emerge. MAOSCO, the international consortium that licenses the MULTOS specification, has committed the next generation of MULTOS to support a Java run-time engine (Cannon & Wooderson, 1999), but only time will tell to what extent the commitment is met.

7.6.15 Public key certification

A different problem relates to public key certification. In testimony before a committee on banking and financial services of the United States House of Representatives on 11 June 1996, Denis A. Calvert Vice President and General Manager United States Financial Retail Division, VeriFone, said,

> "...one of the cornerstones that will shape the future of money is the strength of a private sector national and international Public Key Certification infrastructure (PKI). The foundation for Electronic Commerce in the broadest sense depends on this crucial infrastructure, including many Internet payment schemes. If these certification systems are susceptible to compromise, if they are not supported in law, if they do not provide a solution to the business liability issues related to a Certificate Authority,

then business transactions and the transfer of money over public networks may never reach their full potential". (Calvert, 1996, p. 2).

7.6.16 Holder certification

However, the need for a certification authority goes beyond financial applications. Before any multi-application card is accepted by the public there will need to be a procedure and authority agreed by the issuers of the applications, for determining, at the time card users are enrolled, that they are indeed who they say they are. Similarly, each reader or terminal will need to be certified in some way as being what it purports to be. The certification authority model would need to be agreed nationally or, preferably, internationally ("Curly questions", 1997). An international standard for certificates of this kind has existed for several years, documented within the CCITT standard X509, and services of this nature are being offered in the US, but not yet globally. As mentioned in section 4.3.4, in Australia, SecureNet offers this certification service.

7.6.17 Summary

After taking these difficulties into consideration, one may conclude only that a critical mass in any application, or combination of applications, cannot be expected soon. Incompatibility between smart cards has the potential to delay their widespread introduction for several years. The ongoing struggle for competitive edge and the gaps in standardisation, until resolved, will prohibit the multi-application card that is essential for acceptance. At present there is no compelling pressure that would cause the leading stakeholders to sink their differences and move to a worldwide smart card system. As an editorial in the Australian Computer News put it "Only the foolhardy would expect companies involved in this brand-new technology to work together." ("Scourge", 1997). Having said that, it should be added that amongst the competitors some are more likely to win than others. In the USA, a card system using the Microsoft sponsored PC/SC specification in conjunction with Windows for Smart Cards and finding a market in e-commerce is probably the favourite. In Europe, an application using a mobile phone as a payment terminal with the aid of a smart card might be more likely. Close behind could be ticketing applications using a dual interface card and a modified MIFARE specification, or other protocol acceptable to the financial institutions. Finally, less likely, is the possibility that governments will sponsor a benefit smart card incorporating an electronic purse and with identification established using a biometric feature.

7.7 Industry forecasts

An alternative approach to forecasting the future use of smart cards is to extrapolate from past growth, rather than to evaluate expectations. From reading predictions in journal articles and Internet pages one might easily gain the impression that we will all be familiar with smart cards within a decade. Table 9 follows with estimates or forecasts made by various organisations and authors, some of which approach, and in one case equals, the world population. The most recent short-term forecasts, for 2000, seem to group around two billion cards. However, the "track record" of earlier long-term forecasts suggests that the spectacular increases indicated after 2002 should be regarded with caution. Despite caution, and accepting the doubtful nature of available information, in view of the rapid growth in e-commerce and consumer applications such as PAY-TV, health cards and mobile phones, and bearing in mind the expiry of patents taken out up to 25 years ago, the two billion card forecast does seem plausible. With a world population of six to seven billion, of which less than one billion is in Europe, the forecast implies that almost every breadwinner in the developed world, outside of the US, will carry a smart card. Some caveats would be prudent.

- The probability that affluent sophisticated people may choose to carry more than one smart card must be acknowledged.
- Some authorities, for example, Schlumberger, may disagree with the more optimistic forecasts. In a review published on the Internet in April 97, it estimated that 1.35 billion chip cards would have been issued by the year 2000, but tnat only 450 million of them would be "smart". ("Schlumberger", 1997). In a later forecast for the year 2005, Schlumberger seemed more optimistic, but it should be noted that the information for the longer term forecast is second hand, being a BitCom statement of Schlumberger's opinion.

- There are doubts about the validity of statements even by sources considered more reputable. For example, the Financial Times Business Research Archives issued a WWW page about WHSmith, the bookseller, and use of smart cards, that made the statement, "In 1994, 99% of the 420 million smart cards were...." ("Financial Times", 1997). Since this figure is outside the range of numbers reported for 1996, it can hardly have been true in 1994.

- The fact that two billion cards have been issued does not necessarily mean that they have been activated and in use. As described in sections 7.4.5 and 7.6.9, the actions of HBF and Telstra in Australia have already shown that cards may be issued, but then either not activated, or else only partially exploited.

Generally, it seems that forecasts are ill-defined, and occasionally conflicting, and provide insufficient grounds for disregarding the conclusion in the previous section that there is as yet no existing or imminent compelling pressure to establish smart card systems worldwide.

Table 9A: Schedule of Estimate and Forecast References (1992-1998).

No	Source	Year estimate or forecast made	Reference	Year for which estimate or forecast made	Estimate or Forecast (billions)
1	Baker, T	1992	See references	1992	0.26
2	"CASCADE"	1994	"	1992	0.25
3	"Orga"	1995	"	1994	0.134
4	Cordonnier, V.	1995	"	1994	0.3
5	"Gemplus"	1997	"	1994	0.11
6	Choi & Whinston	1998	"	1994	0.11
7	Goldfinger, C.	1998	Quoting Orga , Gemplus & Philips in Economics of Financial Applications of smart cards p. 9 Obtained from: http://www.ispo.sec.be/fiwg/fasc.htm	1994	0.132
8	Baker, T	1992	See references	1995	1.0
9	"Orga"	1995	"	1995	0.235
10	Cordonnier, V.	1995	"	1995	0.4
11	"Philips"	1995	"	1995	0.052
12	"Solaic"	1997	"	1995	0.04
13	Amdur, D.	1997	"	1995	0.084
14	Goldfinger, C.		Quoting Orga , Gemplus & Philips in Economics of Financial Applications of smart cards p. 9 Obtained from: http://www.ispo.sec.be/fiwg/fasc.htm	1995	0.178
15	Myers, W.	1996	See references	1996	0.35
16	Fancher, C.	1996	"	1996	0.156
17	Benhammou,T	1997	"	1996	0.151
18	Choi & Whinston	1998	"	1996	0.205
19	Frost & Sullivan	1999	Facts & Forecasts Obtained from: http://www.cardlogix.com/factoids.html	1996	0.102
20	Dataquest	1997	GartnerGroup's Dataquest Hot News Obtained from http://www.infopower.com.tw/trend/dataquest/chip-card.htm	1997	0.311
21	Gemplus	1999	Smart Success. Riding high on multiple applications, smart cards are here to stay in the Indian market March 15th, 1999. Obtained from: http://www.dqindia.com/mar1599/ds1.htm	1997	0.9
22	DataQuest	1998	Gemplus edges Schlumberger. Obtained from: http://www.cardtech.faulknergray.com/more.htm	1998	0.3
23	Ovum	1998	Multi-application smart card prospects. Ovum claims. Obtained from: http://www.cardtech.faulknergray.com/more.htm	1998	0.645
24	Philips	1999	BitCom quotes Philips. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	1998	1.362
25	Andersen	1999	Smart cards account for 18% of world card production. Cardtech quoting Arthur Andersen Co. Obtained frm: http://www.cardtech.faulknergray.com/	1998	1.2

Table 9B: Schedule of Estimate and Forecast References (1999-2005).

No	Source	Year estimate or forecast made	Reference	Year for which estimate or forecast made	Estimate or Forecast (billions)
26	"Orga"	1995	See references	1999	1.212
27	"Philips"	1995	"	2000	0.513
28	Daniels, G.	1995	"	2000	0.75
29	Cordonnier, V.	1995	"	2000	1
30	Fancher, C.	1996	"	2000	0.99
31	Benhammou, J	1997	"	2000	1.34
32	Amdur, D.	1997	"	2000	1.1
33	"Soliac"	1997	Excludes Japan and China"	2000	0.4
34	Schlumberger	1997	"	2000	0.45
35	Cordonnier, V.	1997	"	2000	4
36	Goldfinger, C.	1998	Quoting Orga , Gemplus & Philips in Economics of Financial Applications of smart cards p. 9 Obtained from: http://www.ispo.sec.be/fiwg/fasc.htm	2000	1.088
37	Choi & Whinston	1998	See references	2000	2.4
38	"Soliac"	1999	BitCom quotes Soliac. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2000	1.25
39	"Philips"	1999	BitCom quotes Philips. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2000	2
40	"Mentis"	1999	BitCom quotes Mentis. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2000	2
41	"CardTech"	1999	BitCom quotes Card Technology. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2000	2.8
42	"Gemplus"	1999	BitCom quotes Gemplus. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2000	2 to 3.8
43	"Siemens"	1999	BitCom quotes Siemens. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2001	2.8
44	"Dataquest"	1999	BitCom quotes Dataquest. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2001	3.4
45	Ovum	1998	Obtained from: http://europe.cnnfn.com/digitaljam/newsbytes/111910.html	2003	2.7
46	"Gemplus"	1999	BitCom quotes Gemplus. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2003	6.3
47	"Ovum"	1999	Card Technology quotes Ovum. Obtained from: http://www.cardtech.faulknergray.com/more.htm	2004	3
48	Schlumberger	1999	BitCom quotes Schlumberger. Obtained from: http://www.bit-inc.com/htmlfiles/overview.htm	2005	3.75

Before discussing this Table attention is drawn to the following points.

- The published forecasts often do not specifically distinguish between memory cards and true smart cards. The schedule attempts to show only true smart cards and, for example, if the application is known, the following have been assumed to be memory cards not smart cards.
  - Payphone cards
  - Games cards
  - Meter cards
  - Access control cards
  - Vending machine cards

This may be an invalid assumption in some ways because, for example, some payphone cards are true smart cards that are being used in memory card mode.

- The same assumption appears to have been made by the Gemplus forecast published by Cardshow in December, 1995.
- Published information is usually either well dated or second-hand. This is probably because, when up-to-date, it is valuable. For example, Killen & Associates asked US$4,000 for a copy of their 1997 report, "Non-banks' smart card strategies". Other market researchers, DataQuest and DataMonitor, charge similar amounts, and figures attributed to these and similar organisations have been taken from the published material of authors who, it has been assumed, did have access to the original material.

In an attempt to portray the situation more vividly, Figure 18 shows the information graphically. The circles in each row represent either a forecast or an estimated total of smart cards in use in the year given at the left of the row. The years in the bottom row show the years in which the forecasts or estimates were made. The size of the circles approximate to the relative size of the corresponding estimate or forecast, whilst the number within or near each circle refers to the source in Table 9. The circles in Figure 18 are not to scale and attempt merely to give an impression of the relative sizes of the corresponding estimates or forecasts. As may be seen, forecasts, represented by circles above and to the left of the dotted line, have tended to be optimistic and it would be prudent, therefore, to presume that this is still the case. There are sometimes wide variations between estimates: for example, Dataquest (in 1998) estimated there to be 0.3 billion smart cards and Ovum more than twice that number. However, to some extent confidence in the figures is restored by the two most recent confirmable estimates (for 1998) with Phillips reporting 1.36 billion and Arthur Andersen, 1.2 billion.

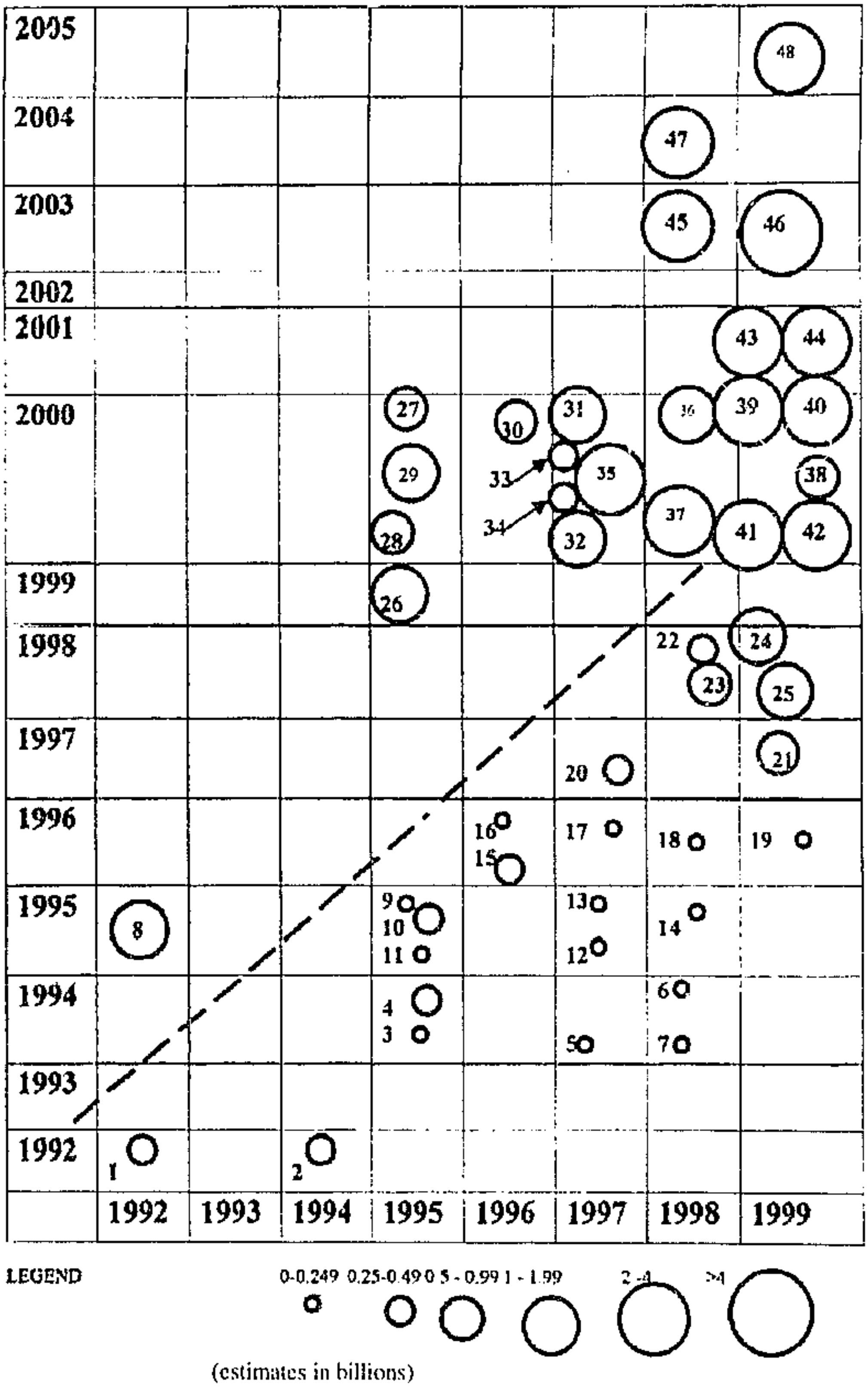


Figure 18: Graphical portrayal of smart card estimates and forecasts.

7.8 Perceived need for better vehicle management

In chapter three it is concluded that a smart card vehicle management system has the potential to improve each of the vehicle management components: namely, traffic management, usage control, maintenance, and security. However, in chapter one it is argued that perceptions rather than reality will be crucial in determining whether a better or more personal system will be adopted. It is the authorities, rather than owners or drivers, that are concerned with traffic management and, as would be expected in democracies, the authorities' ambivalent attitude reflects that of the public. Most people would like better regulation of driving behaviour, and reductions in congestion and pollution, but only if it is others who must modify their behaviour. On balance, despite occasional calls for improvement, there seems to be no strong public perception of a need for change. To have determined objectively how individuals view the need for usage and maintenance control would have required a description of the perceived meaning of the term and a second questionnaire. Instead discussions with friends, and with a contact in the RAC, led to the tentative and unsubstantiated conclusion that most people see the existing arrangements as adequate. For the individual, usage control is subordinate to personal convenience, and maintenance control by windscreen stickers, supported by reminders from service stations, is familiar and satisfactory. Fleet managers view things differently, regarding these components as more important, and their main objection to the available automatic logging systems was cost. The managers that responded to the questionnaire at Appendix 6, would have welcomed a system obtainable at what they regarded as a reasonable figure, but expressed misgivings about the possible reaction of employee drivers. In conversation, for a total system, including both usage control and security, one percent of vehicle cost was mentioned and, as stated in chapter six, this would be about A$200 per vehicle. This modest figure suggests that there is no strong perception of any need for change.

Unlike fleet owners, the main concern for owner-drivers is security. If a smart card security system could be provided at close to the same cost as an immobiliser, then it would probably be chosen because of the extra facilities it would provide. The result of the questionnaire distributed in the University car park suggests that owner-drivers would like better security but would be prepared to pay only from A$100 to A$500 for it.

It seems there is no great pressure for change. If the cost of a smart card system could be brought to within a range acceptable to owners, individual owners might install it to improve security. By contrast fleet owners might be motivated more by a wish to acquire, and have control of, the additional information that could be extracted and would be happy to improve their negotiating position with the oil companies. A possible development that could encourage adoption of in-vehicle smart card systems is robot refuelling ("Robot", 1997).

If all the modifications listed in chapter six were required, the system would be expensive and would have aspects that not all owners would want. No one group of users perceives a need for all aspects, and a general conclusion, therefore, is that an acceptable vehicle smart card management system, should be flexible enough to enable owners to choose only the aspects that they perceive as necessary, and for which they are prepared to pay.

7.9 Conclusion.

The point has been made repeatedly that a probable precondition for smart cards to be used in vehicle management is their widespread use. One day, smart cards may be as ubiquitous as wristwatches and be not just a convenience but a necessity, enabling us to organise our immediate surroundings in at least two ways. First, we may be able to configure the smart card to suit our individual need, thus making each card as unique as its holder, and second, we may be able to personalise the devices around us. A wide range of devices (telephones, vehicles, TVs, dwellings, PCs and others) may be able to accept and read the smart card, and then operate according to our personal preference. Nevertheless, at present there is no clear business case for moving to smart card systems worldwide, because biometric identification cannot meet the more exacting financial institution requirements; and, the ongoing struggle for competitive edge and the gaps in standardisation, until resolved, will prohibit acceptance of the multi-application card. Even outside the commercial world, no killer application has emerged, and forecasts of growth are conflicting and unconvincing. For the motoring world the technology is probably already adequate, but without either widespread use, which depends on the factors already mentioned, or pressure from the public or authorities, the development of smart card systems and their installation in vehicles would cost more than the benefits would justify. The obstacles may eventually be overcome, but the process is likely to be incremental, and a realistic conclusion is that smart cards will not be used to personalise vehicles within the postulated ten-year time frame. With regard to the opening fantasy about summoning and dismissing a car like a magic carpet, it should be noted that the technology already exists. GM has conducted a driverless test on a stretch of highway I-15 in San Diego, California and the French INRIA has conducted a realistic experiment at Saint Quentin en Yvelines using driverless electric cars which the public are able to access using smart cards (Le systeme Praxitele, 1999). Notwithstanding the above, a felt need for the technology does not exist.

Future work should include further investigation of vehicle owner and/or operator attitudes to smart card assisted vehicle management and the investigation of the opinions of both fleet operators and regulatory authorities using a larger, more representative sample. Researchers in a different study discipline could probably better address any follow-up study. Although pertinent, an investigation of possible shifts in commercial intentions might be fruitless, because of the commercial sensitivity of the information, but an investigation of the feasibility of developing a smart card supported vehicle tracking and locating system might be of interest and is planned. The problems of introducing an improved system are not new and it may be appropriate to give Machiavelli the last word.

"There is nothing more difficult to carry out, nor more doubtful of success, ...than to initiate a new order of things. The reformer has enemies in all those who profit by the old order and only lukewarm defenders in those who would profit by the new order." (Machiavelli, 1513, Ch 6, paragraph 4/8).

REFERENCES

Abate, T. (1997, June 3). Thumbs up for finger ID. *The Australian, p.4*

Adams, J. (1993) Car Alarms & Steering Locks Just Don't Work. *Security Australia Vol 13(7).*

Adams, J. (1996). QuikTrak goes back to market with CarWatch *Security Australia Vol 16(3).*

Agre, P. & Harbs, C. (1994) Social Choice About Privacy: IVHS in US. *Information, Technology and People Vol 7(4).*

Allen, C.A. & Kutler, J. (1997). Overview of smart cards and the industry. In Allen & Barr (Eds) *Smart Cards: Seizing strategic business opportunities.* Irwin Professional Publishing, Chicago.

Amdur, D. (1997). *European banks play their (smart) cards.* Obtained from: http://www.byte.com/art/9704/sec18/art1.htm.

Anderson, R. & Kuhn, M.(1996) *Tamper Resistance - a Cautionary Note submitted to USENIX Electronic Commerce, Oakland.* Obtained from: http://www.cl.cam.ac.uk/users/rja14/tamper.html

Arazi, B. (1991) Vehicular Implementations of Public Key Cryptographic Techniques. *IEEE Transactions on Vehicular Technology Vol 40 No 3.*

Arensonas, N. (1996) Self-service electric car rental on the way. *Journal of Advanced Transport Infrastructure. June, 1996. P. 51.*

Ashley, C. (1993) Vehicle security. *Automotive Engineer Vol 18 (5).*

"Australian Economic Indicators". (1997). *Australian Bureau of Statistics, Canberra. ABS Catalogue No 1350.0.*

Babalon, D. (August, 2000). *Hot mobile phone market sparks shipment record.* Obtained from: http://cardtech.faulknergray.com/stor.htm#26.

Baker, T.(1992) Smartcards from a Manufacturer's Point of View. *Solid State Technology.*

Bank of England. (1997). *Bank Notes Fact Sheet Security and Design* Obtained from: http://www.bankofengland.co.uk/fsbnsecu.htm

"Banks Launch" (1997). *Banks Launch First Dual-Chip Identity and Stored-value Smart Card in Asia - Gemplus Provides Smart Card Technology For This Initiative.* Obtained from: http://www.gemplus.com

Bannerjee, R. (1997) Smart card standards and electronic purse. *A review paper.* Aston University, UK.

Barr, W., Allen, C.A. & Burke, J. (1997).Shifting boundaries. In Allen & Barr (Eds) *Smart Cards: Seizing strategic business opportunities.* Irwin Professional Publishing, Chicago.

Barua A., Pinnell J., .Shutter J., and Whinston A., (1998) *Measuring e-commerce.* CISCO, University of Texas. Obtained from: http://www.oecd.org/dsti/sti/it/ec/prod/e_97-185.htm

Battle. (1996). *Battle of the purses.* NEWS RELEASE. Obtained from: http://www.sjb.co.uk/pr/16099601.txt

Bauer, P. & Hamann, U. (1996) *The World in your Wallet.* Siemens Review. Obtained from: http://ptn.wbinet.nl/Siemens/Review/sr9601e.htm

Benemann, T. (1998) *Feds announce collection of information on e-commerce.* ForbesASAP Obtained from: http://www.forbes.com/asap/html/99/0608/feat.htm

Benhammou, J. (1997, September). Recent developments in smart card technology. *Electronics Australia. . p. 30*

"Best practise" (2000, January) *Best practises in testing and reporting performance of biometric devices, Version 1. Biometrics working group.* Association for Biometrics. Obtained from: http://www.afb.org.uk/bwg/bestprac10 .pdf

"Big players" (1999, September 14th) Big players get smart with cards. *The Australian, p. 39.*

Biles, D. & Willing, R. Co-chairmen. (1987). Car Theft: Putting on the Brakes. Proceedings of a Seminar on Car Theft. *NRMA in Assoc with Australian Institute of Criminology.*

Biometrics Ready to Combat Fraud. (1994) *Banking World 12(7)*

Blythe, P.T., Clark, D.J. & Rourke, A.(1994) Results of the Cambridge experiment in congestion management. *Conference Publication No 31. Seventh International Conference on Road Traffic Monitoring and Control.*

Blythe, P., Burdon, M., Clark, D., Givens, J. & Rourke, T. (1994). *The ADEPT Project. DRIVE/ATT Project V2026: ADEPT (Automatic Debiting and Electronic Payment for Transport)* Obtained from: http://www.ncl.ac.uk/~nteng/torg/drive/adept/adept.htm.

Bovelander, E. & Van Renesse, R. (1995). Smartcards and biometrics: an overview. *Computer Fraud and Security, p. 11..* Elsevier Science Ltd.

Brislen, P. (2000) The detail on e-tail. *Unlimited Magazine, May 2000.* Obtained from: http://www.sharechat.co.nz/archives/current/msg00111.shtml

Butler, G. (1996) Why smartcards. *New Zealand Futures Trust.* Obtained from: http://www.itanz.org.nz/pubs/smartcards/smartcards.html

Calvert, D.A. (1996). *Testimony before the Subcommittee on Domestic and International Policy of the Committee on Banking and Financial Services.* United States House of Representatives, June 11, 1996. Obtained from: http://www.house.gov/castle/banking/calvert.htm

Campbell, J.P. & Alyea, L. (1995). *Update on the US Government's Biometric Consortium.* (Obtained from: www.vitro.bloomington.in.us:8080/~BC/REPORTS/CTST95.html)

Campbell, J.P. & Alyea, L. (2000). *Government applications and operations.* (Obtained from: www.biometrics.org/REPORTS/CTSTG96.html)

Camtech, Intellect net sales solution. (1997, November 11). *The Australian* p. 38.

"Can current technologies." (2000). *Can current technologies allay fears over the security of financial transactions on the WWW.* Essay by University of Northumbria. Obtained from: http://www.unn.ac.uk/~i395038/essay.html

Cannon, D. & Wooderson, R.K. (1999). *JTAP586 Project report: Extending the applications of smart cards: Internet cash payment and personal data.* Obtained from: http://www.ex.ac.uk/ECU/mondex/JTAP/J030r.htm

Car running costs. (2001) Obtained from: http://www.rac.com.au/

Carter, R. (1995) Biometric Technology: Progress in Research & Usage. *Datapro Information Security Service.* McGraw-Hill

Car theft. (1997). *Car theft in Eastern Australia 1996.* NRMA Insurance Ltd.

"Car theft action." (1997, May 22). Car theft action urged. *The West Australian.* P. 5.

CASCADE FIRST PRESS RELEASE: 1 MARCH 1994. Obtained from: http://www.dice.ucl.ac.be/~dhem/cascade/press_rel.html#RTFToC1

CASCADE Project Press Release. (1995) Obtained from: http://www.dice.ucl.ac.be/~dhem/cascade/press_rel.html#RTFToC1

Cascade, a new chip generation for smartcards. (1997). Obtained from: http://www.gemplus.com/presse/city_university.htm

Cashless Society: Australian Federal Bureau of Consumer Affairs. (1995). *Electronic Banking and the Consumer.* Australian Government Publishing Service, Canberra.

Castella-Roca, J., Domingo-Ferrar, J., Herrera-Joancomarti, J. & Planes, J. (2000). A performance comparison of Java cards for micropayment implementation. *Proceedings of the fourth working conference on smart card research and advanced applications, September 20-22, 2000. (pp. 225-240)* Bristol, UK.

CCTA Report. (1995, September) *Standards for smart cards.* Obtained from: http://www.itanz.org.nz/pubs/smartcards/smartcards.html

"CEPS" (June 21st, 1999). *CEPS – updated technical specification now obtained.* Obtained from: http://www.europay.com/common/Index.html

"Changing".(1997). Changing the Nature of Money. *New York Times May 9th, 1997.*

Chen, Z. & Kuo, C.H. (1991) A Topology Based Matching Algorithm for Fingerprint Authentication. Conference Paper *Proceedings of the 25th Annual 1991 International Carnahan Conference on Security Technology.*

Chen, Z., Sun, Y., Zhang, Y. & Mu, G. (1995). Hybrid Optical/Digital Access Control Using Fingerprint Identification. *Optical Engineering Vol 34 (3)*

"Chips ahoy". (1997, October 13). *Time Magazine.*

Choi, S-Y & Whinston, A. (1998) *Smart cards. Enabling smart commerce in the digital age.* Center for Research in Electronic Commerce, University of Texas, Austin. Obtained from: http://cism.bus.utexas.edu/works/articles/smartcardswp.html

City Link Project. (1999, October 21st). Obtained from: http://www.citylink.vic.gov.au/pages/home.html.

"Coalition's ". (1996, November 30th). Coalition's $18m car alarm carrot. *The West Australian, p.1.*

Clark, J. (1994). Paying for transport through new technology. *Logistics Information Management Vol 7(6).*

Clark, R.V. & Harris, P.M. (1992) Auto theft and its prevention. *Crime and justice: A review of research Vol 16,* University of Chicago Press: pp. 1-54.

Clarke, R. (1996). Privacy issues in smartcard applications in the retail financial sector. *Commission in 'Smart Cards and the Future of Your Money', June 1996, pp. 157-184*Obtained from: http://www.anu.edu.au/people/Roger.Clarke/DV/ACFF.html

Coetzee, L. & Botha, E. (1993) Fingerprint Recognition in Low Quality Images. *Pattern Recognition Vol 26 No 10,* Pergamon Press Ltd.

Consumer Privacy and Smart Cards - A Challenge and an Opportunity.(1994). *Legal & Public Policy Committee - Smart Card Forum* Obtained from: http://www.smartcrd.com/info/more/privdoc.htm

Corcoran, D., Sims, D. & Hillhouse (1999). *Smart cards and biometrics: your key to PKI.* White paper. Obtained from: http://www.abio.com/whitepapers.htm

Cordonnier, V. (1995). *Using the Smartcard for Money Management & Service Access.* Teal Group International Smartcard Technology Seminar, Perth.

Cordonnier, V. (1997). *The future of smart cards. Technology and applications.* Seminar - Edith Cowan University, Perth.

Costlow, T. (February 3, 2000) *Standard for contactless smart card finds support.* EETimes.com Obtained from: http://eet.com/news/97/965news/contractless.html

"Cutting chips". (1997, September 9). *The Australian, p. 29.*

"Curly questions". (1997, April 29). Curly questions for smartcards. *The Australian, p. 15.*

Daniels, G. (1995). Playing with a full deck. *Communications International Vol 22(8).*

"Dash to digital cash". (October, 1999) The dash to digital cash: enabling internet commerce microtransactions. *Aberdeen Group,* One Boston Place, Boston, MA 02108. Obtained from: http://www.aberdeen.com/ab%5Fcompany/hottopics/digicash/digitalcash.pdf

Davies, H.G. (1994). How biometric technology will fuse flesh and machine. *Information Technology and People. Vol 7 (4).* Obtained from: www.privacy.org/pi/reports/biometric.html

Devery, C. (1993) *Patterns of Motor Vehicle Theft.* NSW Bureau of Crime Statistics & Research, Sydney.

Dhem, J., Veithen, D. & Quisquater, J. (1996). SCALPS: Smart card for limited payment systems. *IEEE Micro Vol 16(3), pp. 42-51.*

Dick, D. (1995) IT Support for Changes in Retail Business. *Petroleum Review June 1995.*

"Digital security." (1998, June 16th). Digital security a smart move. *The Australian, p. 49.*

"Driver's license". (1999) Driver's license cards – identification cards. Obtained from: http://www.aamva.org/aamvanet/indexStandards

Duffy, F.X.(1994) Smart Card Technologies and Markets: Overview. *Datapro Information Security Service Report IS71-100-101*

Duffy, F.X.(1996) Smart Card Technologies and Markets: Overview. *Datapro Information Security Service Report IS71-100-101*

Ely, B. (1996). Electronic money and monetary policy: separating fact from fiction. *Cato Institute.* Obtained from: http://www.cato.org/moneteonf/money14.html

"Electronic Cash" (1995). Electronic cash: Tokens and Payments in the National Information Infrastructure. Obtained from: www.cnri.reston.va.us:3000/XIWT/documents/dig_cash_doc/ElecCash.htm

"Electronic" (2000) Electronic driver licence program. Obtained from: http://www.aamva.net/aamvanet/Driver/appED.html.

"Electronic money" (1997). Chipper for now. *The Economist April 26th.*

"Electronic signatures". (Dec, 1999) Electronic signatures. Signing up to the digital economy. *InterForum white paper number 7.* Obtained from: http://www.interforum.org/frames/frames3.htm

"Electronic Toll Collection" (1997). Electronic Toll Collection. Introduction. *ETC Systems in the. United States, Europe, and Asia.* Barriers to implementation. Obtained from: http://pelican.its.berkeley.edu/PATH/DSS/etc.html

"Facts". (1997, September 16). Obtained from: http://www.fix-the-roads.net.au/facts.html.

"Facts and forecasts." (1999) CardLogix Facts and Forecasts. Obtained from: http://www.cardlogix.com/factoids.html

Fak, V. (1991) Computer Verification of Human Users' Identity: A Theoretical Model & Some Evaluation Criteria. *Computers & Security (10).* Elsevier Science Publishers Ltd.

Fancher, C. (1996). Smart cards. *Scientific American August 1996.* pp 40-45. Obtained from: http://www.jya.com/sacard.txt

Fancher, C. (1997). In your pocket smartcards. *IEEE Spectrum. pp. 47-53.*

Faughnan, J.G. (1999) *International credit card/check card fraud with small charges*: J K Publications, Netfill, Webtel, N-Bill, MJD Services, OnLine Billing, XBC.Com and Charter Pacific Bank. Obtained from: http://www.labmed.umn.edu/~john/ccfraud.html

"Financial Times". Day (1997, July 14). Financial Times Business Research Centre Issue of the Day. Obtained from: http://www.info.ft.com/about/brc/archive/140797.htl

"Fewer". (2000, Feb 3rd). Fewer WA cars stolen. *The West Australian. p. 8.*

Flint, J. (1994) Business is Lousy in Singapore. *Forbes Vol 153 Issue 12.*

Foderaro, L.W. (1998). A test in cashless spending turns out to be a hard sell. *New York Times July 27th, 1988.*

Fox, B.(1995, May 6) ID Cards for a Smart New World. *New Scientist, Vol 146.*

"France Telecom". (Feb 7th, 2000) *France Telecom to turn mobile phone into payment terminal.* Obtained from: http://cardtech.faulknergray.com/stor.htm#36

"Frequently asked questions." (May, 1997) *Frequently asked questions about on-board diagnostics.* United States Environmental Protection Agency: Office of Mobile Sources. Obtained from: http://www.epa.gov/OMSWWW/obd-faq.html

Gates, W. (1996). *The road ahead.* Viking Press, USA.

Gaw, J. & Utting, D. (2000, January 4). US yuletide shoppers spend $US10b online. *The West Australian, p. 38.*

Geason, S. & Wilson, P.R. (1990). *Preventing Car Theft & Crime in Car Parks.* Australian Institute of Criminology.

Gemplus forecasts smartcard market. (1997). *The smart card cyber show.* Obtained from: http://www.cardshow.com/statistics/uk/gemplus.html

"Glossary".(1999). *Glossary of ISO 8583 terms.* Obtained from: http://www.transcan.com/glossary.html.

Goldfinger, Charles (1998) Economics of financial applications of the smart card. *Financial Issues Working group of the European Commission.* Obtained from: http://www.ispo.cec.be/fiwg/fasc.htm

Gottlesfeld-Brown, L. (1992) A Survey of Image RegistrationTechniques. *ACM Computing Surveys Vol 24 (4).*

"Government agencies". (1998, Jan 27th). Government agencies get smart about cards. *The Australian, p. 42.*

Guimmarra, G. & Luk, J. (1995) Proceedings of developments in Paid Parking technologies *Seminar 11 Jul 95 Australian Road Research Board.*

Guthery, S. (2000, April 15th) *Frequently asked questions.* Obtained from: http://www.scdk.com/atsfaq.htm

Hannan, T. (1994). *Information Management in Health.* Paper presented to Smart Cards '94, Sydney.

Hansen, K. (1996). *Ensuring wide acceptance by consumers.* Presentation to ICM Conference on smartcards. March 1996, Sydney.

Harris, P.G. (1992). *Which degree course?* Perth Educational Press, Nedlands.

Harris & Westin (1996) *Equifax/Harris Consumer Privacy Survey.* Obtained from: http://www.equifax.com/consumer/parchive/svry96/docs/summary.html

Harrop, P. (1994). *Charging for road use world-wide.* Financial Times Management, London

Hawryszkiewycz, I. (1998). *Systems analysis and design.* 4thEd. Prentice Hall Australia Pty Ltd.

Haykin, M.E. & Warner, R.B.J. (1988). *Smart Card Technology: New Methods for Computer Access Control.* NIST Special Publication 500-157, US Dept of Commerce.

Hibbert, C. (1996). *What to do when they ask for your Social Security Number.* Obtained from: http://www.cpsr.org/cpsr/privacy/ssn/html/SSN-FAQ.html.

Higgs, M.J. (1996). Smartcards - The key to unlocking revenue growth, Public Transport Electronic Systems. *IEE Conference Publication No 425.*

Hillier, V.A.W.(1988) *Fundamentals of Automotive Electronics.* Hutchinson Education, UK.

Hochholzer, M. (1997) *Present activities and future developments on cryptocontroller smart card ICs.* Obtained from: http://www.bsi.bund.de/literat/tagingsh/hochholz.htm.

Homel, R. (1994). Can police prevent crime? Unpeeling tradition: Contemporary policing. *Centre for Australian Public Sector Management.* Brisbane.

Horngren, C.T. & Harrison, W.T. (1989). *Accounting*. Prentice Hall International, Sydney.

Hottl, W. (1995). *Hitler's paper weapon.* R. Hart-Davis, London

"ICMA Quick card facts". (2000). *ICMA*. Obtained from: http://www.icma.com/info/cardfacts.htm

"ICSA". (1997). *ICSA commercial biometric certification program.* Obtained from: http://www.ncsa.com/services/consortia/cbdc/cbdc-1.html

"In Search". (1997). In seach of the perfect market. *The Economist, May 10th, 1997.*

"InTouch".(1998). In touch #52. *The Smart Card Club.* Obtained from: http://www.smartcardclub.co.uk

Ison, L. (1996). How smartcards impact on the traditional role of the finance sector. *Proceedings of the ICM Conference on "Smart cards". Sydney, NSW.*

"Issues". (1996). *Traffic management: issues and directions [Discussion paper].* Main Roads, WA.

Johnstone, R. (1998, Jul 4th). From Russia with love. *New Scientist Vol 159 (2141).*

"Juiced-up chips". (2000, Jan) *Card Technology News.* Obtained from: http://www.cardtech.faulknergray.com/

Kang, M-C, (1996, Jul 7th). *Smartcard-based system is inherently insecure.* Obtained from: http://home1.pacific.net.sg/~mckang/smartcard.html

Kaplan, J. (1996). *Smart Cards.* The Global Information Passport, International Thomson Computer Press and the CARDTECH/SECURETECH, INC., Conference Proceedings. Obtained from: HREF="http://gsacentral.gsa.gov/sweb/swebt.cgi/0002696/08127 39/SP/viewitem.hml ?18+17+3+0+x+1+x#here"

Kim, H-J. (1995) Biometrics, Is It a Viable Proposition for Identity Authentication and Access Control. *Computers and Security Vol 14 p 205-214.*

Krueger, J. & Schloss, R. (1996) *Facing the Smart Card Security Issue.* Obtained from: http://www.smartcrd.com/info/more/security.htm

Lam, H. & Low-Shang, J.(1994) Smart Cards – Latest Developments in Smart Card Technology. *Phillips Telecommunication Review.*

Lammers, D. (1999, May 7th). *Motorola steers real-time protocol shift for autos. EE Times.* Obtained from: http://www.eetimes.com/story/OEG19990507S0007.

"Law and order". (1996, January 16) *Time Magazine.*

"Le systeme Praxitele". (1999) Le systeme Praxitele – Transport public individuel. Obtained from: http://www-rocq.inria.fr/praxitele/welcome-angl.html

Leach, J (1995) Dynamic Authentication for Smart Cards. *Computers and Security Vol 14 No 5 p385*

Lineback, J. R. (1995) New Uses, Standards May Boost Smartcards. *Electronic Business Today Vol 21 No 12 p24*

Livermore, R. (1993). Attack testing new vehicles. *IEE Colloquium on 'Vehicle Security Systems' pp.9/1-9/3. (Digest No 1993/178). London.*

Luk, J.Y.K. (1995) *Technologies for on-street paid parking. Australian Road Research Board.* Research report ARR No. 263

Lunt, P.(1995) The smartcards are coming but will they stay. *ABA Banking Journal Vol 87(9) p. 46-52*

Lynch, C. (1998) *A white paper on authentication and access management issues.* Coalition for Networked Information. Obtained from: http://www.cni.org/projects/authentication/authentication-wp.html

MacGregor, C.W. (1967). Mechanical properties of materials. *Marks' Standard Handbook for Mechanical Engineers. 7thEd.* McGraw-Hill.

Machiavelli, N. (1513). *Il Principe.* Cambridge University Press, 1988.

MacSmith, D. (1996). *Examining the future of contactless smart card systems.* Presentation to ICM Conference on Smart Cards, March 1996. Sydney.

Mair, Peter (1996) "Consumer payment systems, consumer payment cards;" *Computer Money Day, 28 March; University of Newcastle, Australia.*

Malik, D.F. (1998). *The case for certified wide area road use monitoring.* Obtained from: https://home.earthlink.net~malik/CWARUM/cwarum2.html

Markoff, J. (1996, October 19). Israelis Outline New Risk To Electronic Data Security. *The New York Times, p. 37.* Obtained from: http://ntrg.cs.tcd.ie/mepeirce/Project/Press/sc.html

May, M. (1998, May 23). Whose finger on the button? *New Scientist Vol 158 (2135).*

Mehnert, A.J., Cross J.M. & Smith, C.L. (1994) *Thermographic Imaging: Segmentation of the Subcutaneous Vascular Network of the Back of the Hand.* Research Report 2/93, Edith Cowan University, Perth, WA.

"Microsoft releases."(Nov 22, 1999) Microsoft releases long awaited smart card software. *Card Technology News.* Obtained from: http://www.cardtech.faulknergray.com

"MIFARE PRO" (1997, Oct 1) MIFARE PRO the Dual Interface Card IC Family. *MIFARE NEWS vol -, iss 7, article 7.* Obtained from: http://www-us2.semiconductors.philips.com/publications/content/file_125.html

Miller, B. (1994) Vital Signs of Identity. *IEEE Spectrum, Vol 31 No 2, Feb 1994.*

More about ERP. (2000, February) *More about ERP electronic road pricing system in Singapore.* Obtained from: http://lta.gov.sg/erp/erpwrtup.htm

Motor vehicle theft. (2000, June) *Australian Bureau of Statistics Catalog Number 4510.1.* Obtained from: http://www.abs.gov.au/Ausstats/ABS%40.nsf/b06660592430724fca2568b5007b8619/76c8926bd8a12e1fca2568a9001393f2!OpenDocument

Motor vehicle theft in SA. (1995) *A statistical report from the Comprehensive Auto-theft Research Scheme.* Office of Crime Statistics.

"Motorola-backed ERG". (1997, October 18) Motorola-backed ERG surges back. *The Australian p. 61.*

"Motorola chooses." (1999). *Motorola chooses Atmel for its M-Smart Jupiter smart card platform.* Obtained from: http://www.eu.atmel.com/atmel/news/19990625a.htm.

"Motorola". (1997, March 25th). Motorola set to play its ace card. *The Australian, p. 7.*

"Motorists views" (1996) Motorists views on new cars vehicle safety and technology. *Motoring Directions Vol 2(4)*

Multi-point immobilisers. (1995). Obtained from: http://members.icanect.net/~eahya/new.htm

MULTOS (1997) *The smart card gets smarter.* Press release by MAOSCO Consortium. Obtained from: http://www.multos.com/100.html.

Myers, W. (1996). On trial at the summer Olympic games: smart cards. *Computer Vol 29(7) pp. 88-91.*

Mytec Technologies: Technology. (1996). Obtained from: www.mytec.com/tech/default.htm#optical

MYTEC training: FAQ (1996, Aug 21). Obtained from: http://www.mytec.com/training/chap6.htm#1q01.

Naccache, D. and M'Raïhi, D. (1996) Cryptographic Smart Cards. *IEEE Micro, Vol. 16, No. 3, June 1996.* Obtained from: http://www.computer.org/pubs/micro/backissu.htm#june1996

Noakes-Fry, K (1994) Smart Card Security Applications. *Datapro Information Security Service Report IS71-100-201*

NRI at ABA Solutions '96 Conference. (1997, Feb 10). Obtained from: http://www.nrid.com/96013.html.

O'Loughlin, B.J. (nov 13th, 1998) *Biometrics: An exploration and analysis of user acceptance issuers.* Faculty of Communications, Health & Science, Edith Cowan University, Perth, Ausrtalia.

"Open platform". (2000, December). *Open platform assures interoperability.* Obtained from: http://www.visa.com/nt/suppliers/open/main.html

"OpenCard Framework". (Oct, 1998). OpenCard Framework – General information web document. IBM Deutschland Entwicklung, Boeblingin. Obtained from: http://www.opencard.org/docs/gim/ocfgim.pdf

"Options". (1996) Options for future land transport pricing policy Obtained from: http://www.executive.govt.nz/minister/shipley/ltps/index.html.

Orga cards sold between 1993 and 1995. (1997). *The smart card cyber show.* Obtained from: http://www.cardshow.com/statistics/uk/orga.html

Overview and Applications of Smart Card Technology (1997, Apr 30). Obtained from: http://www.vitro.bloomington.in.us:8080/20g4/smrtcard.html

Owen, R. (1995). What's inside the new breed of smart cards. *Electronics Australia Vol 57(4).*

Paterson, M. (1991) Secure Single Chip Microcomputer Manufacture. *Smart Card 2000.* Elsevier Science Publishers.

Patrikis, E.T. (1996) *Developments on the Management of Foreign Exchange Settlement Risk.* Obtained from: http://www.ny.frb.org/pihome/news/speeches/ep960430.html

PC/SC Workgroup - Overview (1996). Obtained from: http://www.smartcardsys.com/overview.html

PC/SC Workgroup specifications update. (2000, September 11th). Projected release dates for Version 2. Obtained from: http://www.pcscworkgroup.com.

Peyret, P. (1994) *Which smartcard technologies.* Obtained from: http://www.dice.ucl.ac.be/~dhem/cascade/scard95.html

Philips smartcard market by year 2000. (1997). *The smart card cyber show.* Obtained from: http://www.cardshow.com/statistics/uk/philips.html

Phone cards get smarter. (1998, January 13th). *The Australian, p. 32.*

Ponneah, W.D. (1998). *Urban pollution.* Obtained from: http://www.ecard.net/upolltn.html.

"Privacy fear". (1999, October 19th). Privacy fear over ID plan. *The West Australian, p.10.*

Prusa, J. & Reed, S. (1996) Resources - Industry Topics Smart Cards Come of Age. *Journal of Computer-Mediated Communication [On-line], 1 (3).* Obtained from: http://jcmc.huji.ac.il/vol1/issue3/sc2.htm

Rankl, W. and Effing, W. (1997). *Smart Card Handbook.* Giesecke & Devrient GmbH, Munich.

Ratha, N.K., Chen, S. &Jain, A.K. (1995) Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images. *Pattern Recognition Vol 28 No 11. Elsevier Science Ltd.*

Recorded crime in Australia. (1996). Outcome of investigation. *Australian Bureau of Statistics Catalogue No 4510.0.*

Reid, J. & Looi, M. (2000). Making sense of smart card security certifications. *Proceedings of the fourth working conference on smart card research and advanced applications, September 20-22, 2000. (pp. 225-240)* Bristol, UK.

"Robot". (1997, April 15). Robot armed to fill 'em up. *The Australian*

Role of Government in the development and application of smart cards. (April, 1998) *Federation of the electronics industries.* Obtained from: http://www.fei.org.uk/fei/public/position/scgov98.html

Ruggles, T. (1998). A comparisonof biometrics. *Report to the California SFIS.* Obtained from: http://biometric-consulting.com/bio.htm

Rupley, S. (1996). *Digital bucks? Stop here.* Obtained from: http://www.pcmag.com/issues/1510/pcmg0027.htm

Schlumberger Electronic Transactions' Annual Review: An Important Year For Smart Cards. (1997, April 24). Schlumberger Press Release. Obtained from: http://www.slb.com/ir/news/et-review0497.html

"Scourge". (1997, October 21). Scourge of warring standards. *The Australian, p. 34)*

Secure ROM microcontrollers (1999). Obtained from: http://www.atmel.com/products/prod38a.htm

Seidman, S.(1994) TVs to Toll Booths: Smartcard Capabilities. *Security Management Vol 38 No 4*

Sherman, R.L. (1992) Biometric Futures. *Computers & Security (11).* Elsevier Science Publishers Ltd.

"Short description". (2000). Short description of Bluetooth. *The Swede Track System.* Obtained from: http://www.swedetrack.com/usblue1.htm#2

Siemens licenses Java for smart cards.(1997). Smart card market expected to grow wildly, according to company Obtained from: http://www.siemens.de/Al/jw-08-idgns_smartcards.html

Simcoe, T. (1999, April 21) Measuring Business on the Internet: Research and Findings Regarding I-Commerce. *Ernst & Young Center for Business Innovation, One Cambridge Center, Cambridge. Presentation to OECD Workshop on: "Defining and Measuring Electronic Commerce", Paris.* Obtained from: http://www.oecd.fr/dsti/sti/it/ec/act/programme_ECworkshop.htm

"Smart card". (1997, October 14). *The Australian, p. 37.*

"Smart-card makers" (1998, September 1) Smart card makers appeal to Canberra. *The Australian, p 37.*

"Smartcard aims." (1996). Smartcard aims at high volume. *SECURITY: For buyers of products systems & services. Vol 33(4) April, 1996.* Also obtainable from: Industry Veterans Introduce Software Solution to Cut Time, Costs in Card: http://nsi.org/Marketplace/Ads/ubiq.html

Smart Card Factoids. (1996). Obtained from: http://www.smartcrd.com/info/more/Factoid2.htm

Smart card invasion in July. (1997, November 4) *The Australian, p 38.*

Smartcard Developer's Association clones digital GSM cellphones (1998, April 13) Obtained from: http://www.scard.org/press/19980413-01/

"Smartcard Technology". (1994). Smartcard Technology Leading To Multi Service Capability. *Card Europe Smart Card Technology Background Paper* (Obtained from: www.gold.net/users/ct96/rep1.htm)

Smartcards. (1996) *Choice. Feb 1996.* Australian Consumers Association.

"Smartcards in spotlight". (1997, May 19). Smartcards in spotlight at CardTech conference. *Electronic News Vol 43 No 2168. p. 8(2).*

"Smarter Java". (1997, July 15). Smarter Java cards 'aimed at networks'. *The Australian p. 47.*

"Standards set". (1998, May 12th). Standards set for biometrics. *The Australian* p. 54.

Solaic. (1997). *The smart card cyber show.* Obtained from: http://www.cardshow.com/statistics/uk/solaic.html

"Soaring sales" (Jan 2000). Soaring sales of SIM cards could turn into a bonanza. Obtained from: http://cardtech.faulknergray.com/storarc.htm#33.

Sources of State Revenue (1999, February 25th). Obtained from: http://www.audit.sa.gov.au/97-98/staterev.html

South Korean bank to issue multiapplication cards. (2000, Jul 18) *Card Technology Bulletin.* Obtained from :http://www.cardtech.faulknergray.com/more.htm

"Standard Register partners with Schlumberger to improve use and distribution of smart cards." (Sep 25th, 1997). Schlumberger press release. Obtained from: http://www.1.slb.com/ir/news/et-str0997.html

Steinfield, C. (1996). Electronic Commerce: An Introduction to the Special Issue. *Journal of Computer-Mediated Communication [On-line].* Michigan State University. Obtained from: http://jcmc.huji.ac.il/vol1/issue3/genintro.html and http://www.ascusc.org/jcmc/vol1/issue3/genintro.html

Stott, R. (1995) A Happy Invention. *Road Patrol October/November 1995.*

"Study: smartcard". (1997). Study: smartcard market to mushroom. Killen & Assoc. Internet Week October 6th,1997. Obtained from: http://techsearch.techweb.com/se/techsearch.cgi

Students (Preliminary) higher education statistics 2000 (2000). DETYA, Canberra. Obtained from: http://www.detya.gov.au/archive/highered/statistics/student2000shes.pdf

"Sun Microsystems". (1996, October 29). *Sun Microsystems Inc. announces Java card API.* Obtained from: http://www.java.no/presse1196/javacard_api.html

"Sun and Siemens". (1997). *Sun and Siemens ink agreement to embed Java technology into chips for smart cards.* Obtained from: http://www.sci.siemens.com/htdocs/corporate/press/7_22_97.html

Svigals, J. (1996). Opinion: *Smart card: who will seize the opportunity?* Obtained from: http://techsearch.techweb.com/

Svigals, J. (1994) Smartcards - A Security Assessment. *Computers and Security 13 p107-114.*

"TAMPER RESISTANCE". (1996). TAMPER RESISTANCE - A SECOND OPINION by Semiconductor Insights Inc. Obtained from: http://www.semiconductor.com/tamper.html

"Technology/smartcards". (March 1st, 2000). Technology/smartcards frequently asked questions Obtained from: http://www.ioc.ee/atsc/faq.html and http://www.scdk.com/atsfaq.htm

"Telstra winning". (1997, November 11). Telstra winning the smart-card race. *The Australian p. 10.*

Thieves beat car giants. (1996, November 6th). *The West Australian. p. 11.*

"Timorous trade". (1997). Electronic Commerce Survey. *The Economist May 10th. p. 19.*

"Toll road planned for State's north". (1996, November 5). *The West Australian. p. 1.*

Toshiba Introduces Low-Cost Smart Card with 8-bit CPU (12/23/96) Obtained from: http://www.eedesign.com/NewsReleases/Archives/122396.html#2

UniBO Fingerprint Capacitive Sensor. (1997). Obtained from: http://www-micro.deis.unibo.it/~tartagni/Finger/FingerSensor.html.

Wallich, P (June, 1999) Your 0.002 cents' worth. *Scientific Americ June 1999.* Obtained from: http://www.sciam.com/1999/0669issue/0899cyber.html

Wallich, P (August, 1999) How to steal millions in chump change. *Scientific American August 1999.* Obtained from: http://www.sciam.com/1999/0899issue/0899cyber.html

WA Police Annual Crime Statistics Report (1995/96).Australian Bureau of Statistics (WA Office)

Wayner, P. (1998) Cryptographers discuss finding of security flaw in 'smart cards'. *New York Times, June 10th, 1998.* Availab

Wayt Gibbs, W. (May, 1999) The magnetic attraction. *Scientific American May 1999.* Obtained from: http://www.sciam.com/1999/0599issue/0599infocus.html

Wegstein, J.H. (1992) *An Automated Fingerprint Identification System.* NIST, US Dept of Commerce.

Weik, M. (1989) *Communications standard dictionary.* Van Nostrand Reinhold Co. New York.

West Australian Yearbook. (1995) Kelly. P.C. Ed. Australian Bureau of Statistics (WA Office).

West Australian Yearbook. (1996) Kelly, P.C. Ed. Australian Bureau of Statistics (WA Office).

West Australian Yearbook. (1997) Kelly, P.C. Ed. Australian Bureau of Statistics (WA Office).

"What contains" (1995). What contains Smart Card Specifications? *A Frequently Asked Questions List.* Estonian Institute of Cybernetics. Obtained from: http://www.ioc.ee/atsc.

Wigan, M. (1994) The Realizeability of the Potential Benefits of IVHS. *Informnation Technology and People. Vol. 7 No 4.*

Wriston, W. (1996) The future of money. Wriston interviewed by T.A. Bass for *Wired Magazine.* Obtained from: http://www.wired.com/wired/4.10/features/wriston.html

Year Book Australia 1995. (1995) Castles, I. Ed. Australian Bureau of Stastics, Canberra.

Year Book Australia 1996. (1996) McLennan, W. Ed. Australian Bureau of Stastics, Canberra.

Year Book Australia 1997. (1997) McLennan, W. Ed. Australian Bureau of Stastics, Canberra.

Year Book Australia 1998. (1998) McLennan, W. Ed. Australian Bureau of Stastics, Canberra.

Year Book Australia 2000. (2000) McLennan, W. Ed. Australian Bureau of Stastics, Canberra.

Yiacoumi, R. (1997). Will smartcards make the world go round? *Australian Personal Computer. Vol 18(2).*

Zoreda, J.L. & Oton, J.M. (1994) *Smart Cards.* Artech House, Norwood, MA

BIBLIOGRAPHY

Balfour, F. (1993) Wheels of Misfortune: Car Smugglers Bruise Hongkong Insurers. *Far East Economic Review. 25th February, 1993.*

Bennett, L. (1992) New Solutions to Perimeter Protection and Point Access Control. *Conference Paper IEE 1992 International Carnahan Conference on Security and Technology.*

"Car Break-ins: A Growth Industry." (1994 June/July). *The Open Road.*

Crede, A. (1995). Electronic commerce and the banking industry: The requirement and opportunities for new payment systems using the Internet. *Journal of Computer-Mediated Communication [On-line], 1 (3).* Obtained from: http://jcmc.huji.ac.il/vol1/issue3/crede.html

Devargas, M (1992) *Smart Cards and Memory Cards.* NCC Blackwell Ltd. Oxford.

Fingerprint Identification System. (1988). *Paladin Press, Colorado, USA.*

Gill, J.M. (1994) *Standards Committees and Standards Related to Smartcards.* Obtained from: www.gold.net/users/ct96/stds.htm

Guidlines for the Use of Advanced Authentication Technology Alternatives. (1994). *Federal Information Processing Standards Publication 190, NIST, USA*

Harowitz, S. (1993) More Than Meets the Eye. *Security Management Vol 37 No 2*

Harpe, M. de La. (1996) Eye Monitor Doubles as a Warning for Drowsy Drivers. *Campus Review Vol. 6 No. 6*

Harrop, P. (1994) The phantom toll booth: charging for road use. *IEE Review Jan 1994 Vol 44 (1).*

Hill, P. (1994) The Electronic Fingerprint. *Telecommunications International Vol 28 Iss 9.*

Howard, J.A. (1990) Smart Cards. *IEE Colloquium on Vehicle Security 1990.*

Hughes, P.A. & Green, A.D.P. (1991) The Use of Neural Networks for Fingerprint Classification. *Paper presented at the Second International Conference on Artificial Neural Networks at Bournemouth, UK. IEE London UK*

Jurgen, R.K. (1995) The Electronic Motorist. *IEEE Spectrum, March 1995.*

Jurgensen, P.; Larsen, O.V. & Andersen, L.H. (1995) A Model Based Fingerprint Verification System. *Proceedings of a Conference on Shape Structure & Pattern Recognition, World Scientific, Singapore.*

Jusuf, A. (1995). *Users, Programmers and Technical Manuals for Smart Card Access Module and Smart Card Operating System.* Smart Silicon Systems Pty Ltd, Qld.

Kamijo, M. (1993) Classifying Fingerprint Images Using Neural Network. *IEEE International Conference on Neural Networks, Vol 3 p 1932-7, IEEE NY, USA*

Khanna, R. & Shen, W. (1994) Automated Fingerprint Identification System (AFIS) Benchmarking Using the National Instute of Standards & Technology (NIST) Special Database 4. *Proceedings of the IEEE 28th Annual International Carnahan Conference on Security Technology. IEEE, NY, USA*

Kobayashi, T.(1992) A Fingerprint Image Recognition Method for Networ User Identification. *Proceedings of the Fourth International Conference on Computing and Information. IEEE Computer Society Press, USA.*

LaPedus, A. & Andrews, M. (1993) PCs Catch Criminals Using Fingerprint Analysis. *Byte October, 1993*

Le systeme Praxitele. (1999) Obtained from: http://www-rocq.inria.fr/praxitele/welcome-angl.html.

MacLellan, A. (1996) Microchip Introduces HCS300 & HCS301 Code Hopping Encoders. *Electronic News Vol 24 No 2109 p70*

McCrindle, J. (1990) *Smart Cards.* IFS Ltd, Kempston, UK

Margo, J. (1996) How Organized Crime is Hijacking South Africa's Recovery. *The Australian, Saturday 15th June, 1996.*

Mehnert, A.J., Cross J.M. & Chia K.Y.(1995). *A Personal Biometric ID System Based on Back-of-Hand Veins.* AISAT Research Report 1/95.

Mehtre, B.M.(1993) Fingerprint Image Analysis for Automatic Identification. *Machine Vision Applications. Vol 6 p 124-139.*

Moscinska, K. & Tyma, G.(1993) Neural Network Based Fingerprint Classification. *Paper presented at Third International Conference on Artificial Neural Networks at Brighton, UK. IEE London UK*

O'Gorman, L. & Nickerson, J.V. (1989) An Approach to Fingerprint Filter Design. *Pattern Recognition Vol 22 No 1 p29-38*

Pinkerton, J. (1994) Mobile Electronics Wrap-up. *Dealerscope Merchandising Vol 36 Iss 2.*

Prebble, M. (1990) *Integrated Circuit Cards.* Victoria University Press, Wellington, NZ.

Redfern, S.W. (1993) A Radar Based Mass Movement Sensor for Automotive Security Applications. *Conference Paper. IEE Colloquium on Vehicle Security Systems. (Digest 1993/178)*

Rice, J. & Goodwin, B. (1990) Biometric Access and Use Systems. *IEE Colloquium on Vehicle Security 1990.*

Richards, D.R. (1995) Rules of Thumb for Biometric Systems. *Security Management Oct 1995*

Richards, D.R. (1994) ID Technology Faces the Future. *Security Management Vol 38 No 4.*

Shan, Y., Shi, P. & Li, J.G. (1994) Fingerprint Preclassification Using Key Points. *Proceedings of an International Symposium on Speech, Image Processing & Neural Networks. IEEE, NY, USA.*

Sherizen, S. (1995) Can Computer Crime be Deterred? *Security Journal 6 p177-181.* Elsevier Science Ireland Ltd.

Sherlock, B.G.; Monro, D.M. & Millard, K. (1994) Fingerprint Enhancement by Directional Fourier Filtering. *IEE Proc.- Vis. Image Signal Process. Vol 141 No 2.*

Sims, D. (1994) Decriminalizing the Fingerprint. *IEEE Computer Graphics and Applications Vol 14 Iss 4 p15-16.*

Simpson, L (1994) The Fingerscan Personal ID System. *Silicon Chip 7(5), p8-9*

Smartcards: Motorola Adds Further Security Layer to Smartcards. (1996). *EDGE Workgroup Computing Report. Vol 6 No 290 p 11*

Smartcards: Motorola Wins Two European Smartcard Contracts. (1996). *EDGE Workgroup Computing Report. Vol 7 No 302 p22*

Sparrow, M. & P. (1985) *A Topological Approach to the Matching of Single Fingerprints.* National Bureau of Standards, US Dept of Commerce.

Standard Register partners with Schlumberger to improve use and distribution of smartcards. (September 25, 1997). Obtained from: http://www.slb.com/ir/news/ct-str0997.html.

Svigals, J. (1985) *Smart Cards. The Ultimate Personal Computer.* MacMillan, NY.

Traffic Board of Western Australia. (1994). *Annual Report.*

Truly Digital. (1994). *The Economist Vol 331 No 7864*

Unisys Wins Spanish National Welfare Smartcard Deal. (1996) *NEWSBYTES Jan 24th, 1996.*

Vandewalle, J-J.(1995) *Cours Cartes a Microprocesseur.* Departement Informatique. IUT "A" De Lille.

Vedder, K. (1992) Smart Cards. *Proceedings of Comp Euro'92. IEEE Computer Society Press.*

Wayner, P. (1997) *Digital cash.* London: Academic Press Ltd.

Weber, D.M. (1995) A Cost Effective Fingerprint Verification Algorithm for Commercial Applications. *Proceedings of 1992 South African Symposium on Communication and Signal Processing. IEEE Computer Society Press.*

Western Australian Police. (1995/96). *Annual Crime Statistics Report.*

Williamson, Hon Maurice, NZ Minister of Transport, National Road Pricing Study Discussion Paper Released 27 July 1995 Obtained from: httm://www.gov.nz/politics/bio/Williamson.Maurice/roadprice270795.htm

Xiao, Q. & Raafat, H. (1991) Finger Image Postprocessing. *Pattern Recognition Vol 24 No 10.*

Zhang, T.Y. & Suen, C.Y. (1984) A Fast Parallel Algorithm for Thinning Digital Patterns. *Communications of the ACM, Vol 27 No 3.*

Appendix 1

ESTIMATE OF THE PROPORTION OF CARS AND LIGHT COMMERCIAL VEHICLES IN WESTERN AUSTRALIA THAT ARE FLEET OWNED

This proved to be a surprisingly difficult figure to estimate. Enquiries were made of the following organisations:

Australian Bureau of Statistics

Motor Trade Association of WA

RAC

but they were unable to help.

There are about one million cars and light commercial vehicles now registered in WA. New vehicle registrations of these vehicles are now about 50,000 each year. Since the total number of registrations for the last five years has increased by only 25,000 each year it seems that about 25,000 are taken out of use annually.

Senior salesmen in various large dealerships had kept no figures but gave estimates of the proportion sold for fleet use as from 50 to 70 percent. If 60% of new registrations each year are for fleet owners this is 30,000 vehicles. If fleet vehicles are used for an average of three years only before being sold to private owners some 90,000 of WA's light vehicles are fleet vehicles. This amounts to about nine percent. A call to the Federal Chamber of Automotive Industries, Canberra, elicited the verbal opinion that of Australia's eight million vehicles, one million were fleet owned. Ten percent has therefore been adopted as a reasonable "ball park" figure.

Appendix 2

THE CRIME ENVIRONMENT

Efforts to improve vehicle security are a small (perhaps, relatively unimportant) part of society's efforts to reduce crime generally. Crime statistics are capable of different interpretations and these interpretations depend on the weight given to various factors such as policing strategy, media attitudes and public perceptions. Trends in crime differ by categories.

- In WA, total crime seems to be decreasing but crimes against the person are on the increase. (WA Yearbook, 1997, p. 108). For example, for the years 1992-96, total reported crime, excluding vehicle theft, fell: although, violent crimes such as robbery and assault rose (WA Yearbooks, 1995-7). While vehicle theft decreased from 1995 to 1996 over the longer term it has increased. (WA Yearbook, 1996, p. 110).

- Police strategy may distort the figures, although there appears to be little evidence to support that possibility. In the latest yearbook it is shown that for offences against the person the percentage of offences cleared is 82%, whereas for crimes against property it is 21%, but this outcome could be merely a consequence of the fact that there is nearly always a witness to a violent act. Even if suspicions about the statistics are well founded, the number of reported thefts of insured items would probably not be affected because the owner can only claim the insurance if the alleged offence is reported to the police.

- However, it may be that the police, perhaps rightly, devote more resources to the prosecution of violent criminals and that a rise in such crimes, without a compensating increase in police resources, may necessarily result in a relative neglect of crimes against property and a distortion of the statistics.

- Those who support any such strategy argue that crimes against property (of which vehicle theft and theft from vehicles is a component) do not merit the same level of deterrent effort as crimes against the person.

- The counter perception is that if minor crimes rarely result in apprehension, criminals become bolder and commit more serious offences. Civic authorities in New York, where a vigorous campaign has been waged against minor offenders such as drunks, marijuana smokers and vandals, apparently take this view. According to a Time magazine report the campaign has led to a significant fall in all crime including major offences (Law and order, 1996, p. 50). In July 97 there were television news reports of the adoption in WA of a "zero tolerance" policy that appears to bear some resemblance to the New York campaign - although, equally, it could be merely lip service.

- Press reports often point out that crime generally is decreasing but also usually emphasise the increase in crime against the person. Perhaps because of these reports, there is a public perception that overall crime is increasing although the greatest outrage is expressed about crimes against the person.

At the least it can be argued that motorists should not be tolerant of vehicle theft merely because their insurance covers them against major loss.

Appendix 3

VEHICLE THEFT

Larger vehicles are often pillaged but seldom stolen. Over the three year period 1993-1996, in Western Australia, about 1.6% of registered vehicles or an average of nearly 19,000 vehicles each year were stolen at an estimated cost of over $100 million (WA Police Annual Crime Statistics Report 1995/96). In most years WA has the highest rate of vehicle theft in Australia, but figures published recently on the Australian Bureau of Statistics web site show a reduction in the rate. During 1999, the number of motor vehicle thefts in Australia declined by 1.3%, from 131,587 in 1998 to129,865 in 1999. The largest percentage decrease was recorded in Western Australia, where the number of motor vehicle thefts decreased by 21%, from 16,115 in 1998 to 12,752 in 1999 (Motor vehicle theft, 2000). Presumably the community would still welcome any measures to reduce the loss.

Other points obtained from an earlier study by Devery follow (Devery, 1993). Any figures related to car thieves must be regarded with caution since most thefts do not result in the thief being apprehended. In 1988, in NSW, the clearing-up rate (thief apprehended) was 2.74% (Geason & Wilson, 1990). Devery states that only about 5% of car thieves are apprehended (Devery, 1993). In WA, in 1994 - 1995 the rate was 15.9% and in 1995 - 1996, 17.5%. A statistical report from the Comprehensive Auto-theft Research Scheme (CARS) of South Australia, implies a 10% apprehension rate (about 10,000 cars stolen each year and about 1,000 persons apprehended) (Motor vehicle theft in SA, 1995). Finally, a recently published report from the Australian Bureau of Statistics has a table for motor vehicle theft 'Outcome of investigation' which shows the proportion of offenders proceeded against. The figures range from Tasmania 2.6% to Queensland 15.2%. Figures were not available for WA (Recorded crime in Australia. 1996, ABS Catalogue Number 4510.0). Mindful that figures are drawn from the small "selected" sample of apprehended offenders, there is still some evidence that car thieves fall into two broad categories:

• young (under 21)	60%
• older	40%

The profile of a typical car thief is that of a male, aged 14 to 25 and with the mode at age 16. It may be that older thieves have become more cunning and are apprehended less frequently. The situation seems to be long standing, since as far back as 1984 only 15% of car thefts were cleared (Biles & Willing, 1987, p. 42).

In SA about 80% to 90% of stolen cars are recovered within a week (Motor vehicle theft in SA, 1995). This, according to local industry opinion is similar to the situation in WA. Recovery rates in the eastern states are less, varying from 65% to 76% (Car theft, 1997). Probably, therefore, in WA, no more than 20% of those stolen are stolen for resale, either as complete vehicles or as parts. A few (18.7% in SA in 1995) of the proportion quickly recovered will have been stolen to use in the commission of another crime; for example, as a getaway car or for "ram-raid" use. Of the remainder, most are likely to have been taken for joy-riding or for instant temporary transport. One may speculate that for some young people, car theft is a crime much as apple stealing used to be some years ago. Mostly, it is not for profit but is exciting and not particularly risky. It may be a training ground and recruitment area for more serious criminals, but there is no hard evidence to support this. The joy-riding may be on the increase because, in 1993, Devery estimated:

- Short-term use. (e.g. joy-riding, a cheap taxi or to facilitate a more serious crime) 50-60%
- Profit (e.g. for resale or sale as parts) 30-40%
- Fraud (e.g. to collect the insurance) 4-12%

Similar figures are given by Geason (Geason & Wilson, 1990, p. 6).

Older vehicles are more commonly stolen. Devery gives figures that put the average age of stolen cars as between 5 and 15 years with the peak at about ten years (Devery, 1993). The CARS study, however, gives the highest rates of theft for vehicles in the 15 to 18 years age group (Motor vehicle theft in SA, 1995). Popular makes appear to be the most commonly stolen, the five with the highest theft rate per ten thousand vehicles being, in descending order, Holden, Chrysler, Ford, Mazda and Toyota. There is a bias towards bigger, more powerful models. Although statistics show that older vehicles are more often stolen, there have been recent thefts of newer cars that use fairly sophisticated, transponder-supported locking. About 300 such vehicles were stolen in Victoria in late1995, which may have been a transitory anomaly (Thieves beat car giants, 1996). Nevertheless, It would seem highly desirable to develop devices that can be fitted as a kit to an older vehicle. The average age of registered vehicles is also about ten years (Yearbook Australia, 1997, p. 526).

Both Devery and Geason estimate that from 10 to 15% of stolen vehicles were left unlocked. Geason reports that about 5% had the keys left in them. Actual figures quoted by different investigators vary, but it seems that in up to 30% of car thefts the vehicle was either left unlocked or the thief had access to the key or a duplicate

(Motor vehicle, 1995, p.75). In Australia, in about 5% of thefts the keys were left in the car (Geason & Wilson, 1990). In SA in 1995, in 15.4% of vehicle thefts the thief had access to a key and in 14.3% the vehicle was unlocked. Clearly a device that compensates for human carelessness would be useful. According to the CARS study, when thieves forced access, in 43.8% of known cases the lock was manipulated (presumably by driving a sharp instrument through the door panel) and in 19.3% of cases a window was broken (Motor vehicle, 1995, p.75). The most recent study, the NRMA report on Car Theft in Eastern Australia, 1996, does not record the means of entry (Car Theft, 1997). The matter is summarised by Livermore of the UK Police Science Development Branch who writes, "Cars are stolen not because thieves posses fine engineering skills but because they exploit weaknesses in the system. Their approach is... based on familiarity and brute force methods. (They) ... rely on the fact that when they lay hands on a car it is known to them, they know exactly where the weaknesses are: success is certain because they have done it before." (Livermore, 1993).

Statistics are available showing the places from which cars are most commonly stolen but, unfortunately, there are no comparative statistics to show where vehicles are commonly parked. About 30 cars each year are stolen from the Mount Lawley campus car park. With 1500 parking spaces, this is in line with the State average. One gains the impression that unattended, parked cars are stolen impartially from places to which the public have access, including car-parks, kerb-sides and driveways.

Appendix 4

ESTIMATING

GLOBAL MONETARY FLOWS

Cash payments. Within finance there are at least two areas in which smart cards might have a major impact, of which one is the small change, or cash transaction market, already defined. There are varying estimates of its size.

- Choice magazine estimates that, worldwide, the small change market of private expenditure, the market for the electronic purse, (that is, transactions below US$15 in value) is worth an estimated US$1.8t each year (Smartcards, 1996).
- Allied, an organisation conducting market surveys, estimate the total as US$8.1t (Prusa & Reed, 1996).
- Jean McKenna, vice president of Visa International, cited research that, "in the top 29 countries in 1995, more than US$8.1t was spent in cash, 22% for transactions of ten dollars or less" (Myers, 1996). Since 22% of US$8.1t is US$1.782t, McKenna appears to confirm the Choice Magazine estimate.
- An article in the Australian Personal Computer stated that Mastercard believed that money stored on smart cards could one day be worth US$2t (Yiacoumi, 1997).

- A web page quotes a paper by Jack M. Kaplan that, "cash transactions under US$20 are valued at US$2t each year and represent 80 percent of cash transactions." (Kaplan, 1996).
- A recent report to Congress from the US Federal Reserve board on the subject of stored-value cards, stated that transactions of less than US$20, for things like fast food and Slurpees, amount to more than US$500b annually. Credit card companies have already largely exhausted Americans' ability to buy US$75 items on credit cards, but issuing stored-value cards would allow the companies to become involved in the high volume, low price transaction business ("Changing", 1997).
- According to the Bank for International Settlement, the number of consumer cash transactions in the U.S. alone exceeds 300 billion per year. By contrast, bank-facilitated consumer transactions, such as credit and debit cards, cheques, and wire transfers, total only 60 billion per year. The worldwide market for automating cash transactions remains virtually untapped.

Clearly, although there is room for dispute about market size, the figure is substantial. This is an area in which electronic money, possibly facilitated by smart cards, might gain some acceptance. In New Zealand it is estimated that 70% by volume of all transactions are by cash, although cash accounts for only 30% of their value, because the average value of cash payments is less than NZ$10 (NZ Bankers Association Annual Report, 1996; Butler, 1996). By contrast, in Australia, 90% by volume of transactions are still by cash (Mair, 1996). The forgoing figures give an indication of the potential market in which the purse, or other form of electronic money, might be sold. After allowing for growth, the current total might be US$10t.

E-commerce. Steinfield, writing in the Lansing State Journal, 26 December, 1995 claims that in 1994, a consulting firm, Euromonitor, noted that the "global shopping" market was approximately US$166b, and contrasted this with "electronic shopping" that was a mere US$300m (Steinfield, 1996). The terms were not defined. In 1997, an Australian Internet services company, Camtech, asserted that e-commerce was currently A$2b annually, but would grow to A$50b annually by the year 2000 ("Camtech", 1997). In 1998, researchers at the University of Texas, estimated Internet commerce to be US$102b (Barua, Pinnell, Shutter & Whinston, 1998). The figure probably includes Internet shopping. In the same year, Tom Benemann, of Forbes ASAP, estimated the market, exclusive of Internet shopping, to be US$43b (Benemann, 1998). In 1999, Ernst & Young, in a presentation to an OECD conference in April, quoted estimates of e-commerce from various market surveyors that varied from US$9.9b to US$97.2b (Simcoe, 1999). Finally, in a White Paper dated 7 December, 1999, the UK InterForum quoted the IDC, a leading international research organisation, as predicting that e-commerce would rise to US$600b in 2001 and to US$1.1t the following year (Electronic signatures, 1999). These figures, although not always so defined, are assumed to be annual and are summarised in the following table.

Table 1: E-commerce market size

Source	Estimated Actual		Forecast	
	Year	Amount	Year	Amount
Euromonitor	1994	US$300m		
Camtech	1997	A$2b	2000	A$50b
University of Texas	1998 1999	US$102b US$170b		
Forbes ASAP	1998	US$43b		
Goldfinger	1998		2002	US$300b
Ernst & Young	1999	US$9.9 to 97.2b		
InterForum	1999		2001 2002	US$600b US$1.1t

The estimates of its size are increasing, and a reasonable guess at its present size might be US$210b.

E-shopping. In the US, in 1994, the 3.5 million people connected to the Internet spent an average of under 60 cents each via their PCs, compared to US$94 through traditional mail ordering (Steinfield, 1996), but, surprisingly, in 1999 this may have risen. According to Gaw and Utting, writing in the West Australian and quoting the Boston Consulting Group, the per capita global e-tail expenditure in that year was US$60 (Gaw & Utting, 2000). Brislen, writing in Unlimited Magazine in May, 2000, also quoting the Boston Group, gives the figure for the US alone as US$134.20 (Brislen, 2000). The Boston Group cannot be quoted directly because they release their findings only to subscribers. In 1994, according to Steinfield, electronic shopping, including CD-ROMS, accounted for just US$300m in sales, or less than 0.02% of total shopping. Verifone estimated e-shopping in 1994 as a mere US$100m (Hansen, 1996). Gaw and Utting, in the article already quoted, gave the total as

US$40b. However, even discounting the figure from Gaw and Utting, there are hopes for the future. For example, Mondex, in its December, 1996 magazine, stated that payments over the Internet amounted to US$500m, but estimated that by the year 2000 the figure would be in billions. According to the Smart card Forum, Killen and Associates say there were 250 million transactions in 1996 and that this will grow to 25 billion by 2005 (Smart Card Factoids, 1996). A Forrester Research study on Internet commerce, claimed worldwide revenues from interactive, online sales increased from US$240m in 1994 to US$350m in 1996, and could reach US$6.9b by 2000 (Rupley, 1996). In an article in the Economist, Christopher Anderson wrote, "...analysts reckoned that consumer Internet transaction in 1996 were worth ...US$500 - 600m" (Anderson, 1997). He did not identify the analysts, but quoted International Data as forecasting that by the year 2000 consumer online shopping would amount to US$16.1b. These disjointed estimates of the shopping market are summarised in the following table.

Table 2: E-shopping market size

Source	**Source date**	**Sales Estimates**		**Forecasts**	
		Year	**Amount**	**Year**	**Amount**
Steinfield	1996	1994	US$300m		
Verifone	1996	1994	US$100m		
Mondex	1996	1995	US$500m	2000	Billions
Forrester	1996	1994	US$240m		
		1996	US$350m	2000	US$6.9b
Anderson	1997	1996	US$500-600m		
International Data	1997			2000	US$16.1b
Gaw & Utting	2000	1999	US$30-40b		

Forecasting is not an exact science! The larger figures are hardly believable since, if true, they indicate that individual purchases could be equal to one third of business-to-business commerce, and not all forecasters are completely optimistic. For example, Brislen quotes Forrester Research as predicting that "many e-tailing ventures will fail and most will disappear by 2001" (Brislen, 2000). A plausible guess at the total in the year 2000 might be US$10b.

Appendix 5

SYSTEM REPOSITORY

External entities

EXTERNAL AUTHORiTIES
VEHICLE OWNER
VEHICLE
MERCHANT OR SERVICE PROVIDER
DRIVERS/USERS

Data stores

Name	bytes
ArmingCode	2
DriverAuthSupplied	8-256
DriverDetail	68-316
DriverRecord	400
ExtAuthDetail	200
LicenseDetails	60
OwnerDetails	58-306
PersonalisationData	200
Purse	200
SensorReadings	300
ValetCodes	20
ValetOpConditions	10
VehicleDetails	100
ESTIMATED TOTAL	**2400**

Processes

Estimated non-volatile memory required to store code

1 StoreStaticData

(no storage required- process carried out using a terminal emulator)

Get ValetCodes
Get ArmingCode
Get PersonalisationData
Get VehicleDetails
Encrypt ValetCode + ArmingCode
Store ValetCodes
Store ArmingCode
Store PersonalisationData
Store VehicleDetails

```
2.1     EnrolOwner                                                          "
            Get OwnerDetails
            Store OwnerDetails

2.2   EnrolDriver                                                           "
            Get LicenseDetails
            Get DriverDetails
            Get EnrolAuthData
            Get OwnerAuthSup
            Get OwnerEnrolAuthData
                If OwnerAuthSup in OwnerEnrolAuthData then
            Store LicenseDetails + DriverDetails +OwnerID
            Encrypt DriverEnrolAuthData
            Store DriverEnrolAuthData

2.3     EnrolExternalAuthorities                                            "
            Get ExtAuthDetails
            Get OwnerAuthSup /*[Bio|PIN|Password]*/
            Get OwnerEnrolAuthData /*[Bio|PIN|Password]*/
                If OwnerAuthSup in OwnerEnrolAuthData then
            Store ExtAuthDetails  /* a matrix that assigns queries to authorities */
        Note: Above processes would be carried out at an enrolment workstation.

3.1     IdentifyQueryingAuthority                                           200 bytes
            Get ExternalAuthCode + ExternalAuthQuery
                {from transceiver}
            If ExternalAuthCode in ExternalAuthDetail then
                Get ResponseDefinition
                If  ExternalAuthQuery in ResponseDefinition then
                RespondToExternalAuthority (ResponseDefinition )

3.2     RespondToExternalAuthority (ResponseDefinition)                     600 bytes
            If  LicenseDetails in ResponseDefinition then
                Get LicenseDetails
                Send LicenseDetails to transceiver
            If SensorReadings in ResponseDefinition then
                Get SensorReadings
                Send SensorReadings to transceiver
            If Payment in ResponseDefinition then
                PurseBalance :=  PurseBalance - TransactionAmount
                Send TransactionAmount to transceiver
        Note: Above two processes initiated by transceiver signal

3.3     PayForItems                                                         400 bytes
            Get payment from reader
            PurseBalance := PurseBalance - Payment
        Note:  Above process triggered by smart card insertion into a purse wallet or
                cash receiver.
```

```
3.4    AddCashToPurse                                                   400 bytes
           Get CashInput  /* from ATM dispenser */
           PurseBalance := PurseBalance + CashInput
       Note: Above process triggered by insertion into ATM cash dispenser.

4.1    PollVehicleSensors                                               400 bytes
           Get SensorReadings                              Queue structure required
           StoreSensorReadings
       Note:  This process performed at each pulse

4.2    StoreSensorReadings
           /* Process not elauorated. Some items would be overwritten at each pulse.
           Some would be stored at specified event . For example, time of start, at
           start, in a queue of, say, ten.  Speed and deceleration might be stored in a
           queue of, say, 60 items at one second intervals  */
                                                                         2000 bytes
                                                           Comparison required for
                                                            each item

5.1    ValidateDriver                                                   600 bytes
           Get DriverAuthSupplied /*[Bio|PIN|Password]*/
           Get UsageCode
           Store DriverAuthSupplied  /* record last attempt */
           Store UsageCode in DriverRecord
           Get DriverAccess
           Decrypt DriverEnrolAuthData
           If  DriverAuthSupplied in DriverEnrolAuthData then
               ArmVehicleSystems(DriverID)

5.2    ArmVehicleSystems(DriverID)                                      400 bytes
           Get ArmingCode   (*from ArmingCose store*)
           Decrypt ArmingCode
           Send ArmingCode to vehicle microcontrollers
           Get Time (*internally generated*)
           LastStartTime := Time
           Store DriverID + LastStartTime in DriverRecord

5.3    Set ValetMode                                                    400 bytes
           Get ValetSetSupplied  (*as chosen by owner from ValetCodes - can be
                                   ValetSet or ValetReset*)
           Get OwnerEnrolAuthData /*[Bio|PIN|Password]*/
           If OwnerEnrolAuthData = DriverAuthSupplied and then
               Store ValetOpConditions (*can be null when reset*)
               ValetSet/ResetVehicleSystems

5.4    ValetSet/ResetVehicleSystems                                     600 bytes
           Get SensorReadings
           Get ValetOpConditions
```

```
        If ValetOpConditions include Reset or ValetOpConditions less than
            SensorReadings then
                    Get ValetDisarmingCode
                    Issue ValetDisarmingCode to microcontrollers
        Else Get ValetArmingCode
                Issue ValetArmingCode to microcontrollers

6.1     ValidateQueryer                                                  600 bytes
            Get OwnerQuery
            Get OwnerAuthSupplied
            If OwnerAuthSupplied in OwnerEnrolAuthData then
                Get DataRequired
            ExtractData (DataRequired, RequiredData)

6.2     ExtractData (DataRequired, RequiredData)          Search and comparison
                                                           required for each item
                                                                        2000 bytes
            If SensorReadings in RequiredData then
                Get SensorReadings
                Display SensorReadings

7.1     ManageEngine                                                     400 bytes
            Get EngineManagementCriteria
            Get SensorReadings  /* Power and rpm */
            If SensorReadings <> EngineManagementCriteria then
                AdjustThrottleSetting  /* Process not elaborated */

7.2     PersonaliseSeating&Mirrors                                       600 bytes
            Get PersonalSettings /* Required seat and mirror setting */
            Get SensorReadings   /* Actual seat and mirror setting */
            If SensorReadings <> PersonalSettings then
                AdjustSeat&Mirror  /* Process not elaborated */
```

Total storage required for code   9600 bytes

Data flows

	Data structure		Components	Est Storage (bytes)
	Acceleration/deceleration	=	*sensor report*	2
	ActualEngineReadings	=	*Sensor reports of EngineRevs , Temperature, OilPressure, IntakeManifoldPressure, ThrottleSetting*	50
	ActualPersonalSettings	=	*alias PersonalSettings*	
	AppropriateSensorReadings	=	*readings selected for report to external authority*	
	AppropriateVehicleDetails	=	*details selected for report to external authority*	
	ArmingCode	=	*Code to activate designated microcontrollers*	2
	AuthenticationFromDriver	=	*alias DriverAuthSupplied*	
	AuthorisedData	=	*data that may be supplied in response to a query*	256
	BloodGroup	=	*driver's blood group (see DriverPublicHealthDetail) *	3

	CashInput	=	*sum added to purse balance*	2
	Category	=	*(see LicenseDetails)*	10
	Conditions	=	*(see LicenseDetails)*	2
	DataInAccordanceWithAppropriateDefinition	=	*[DriverData | LicenseData}*	256
	DataRequired	=	*(alias QueryDataRequirement or OwnerQuery - Data as specified by the owner)*	256
	Date (Valet set)	=	*(see ValetOpConditions)*	6
	DisplayedDirections	=	*May not involve smartcard*	
	Distance (Valet set)	=	*(see ValetOpConditions)*	2
	DOB	=	*(see LicenseDetails)*	6
	DriverAccess	=	DriverID + DriverEnrolAuthData	
	DriverAuthSupplied	=	[PIN | TransponderSignal | BioTemplate]	8 - 256
	DriverDataInAccordance WithAppropriateDefinition	=	*Data that owner has authorised for release to external authorities*	
	DriverDetail	=	DriverAccess + DriverName + DriverPublicHealthDetails + LicenseNo	
	DriverEnrolAuthData	=	[PIN | TransponderSignal | BioTemplate]	8 - 256
	DriverID	=	*(see DriverDetail)*	2
	DriverJourney	=	DriverID + UsageCode + LastStartTime	
	DriverName	=	*(see DriverDetail)*	30
	DriverPublicHealthDetail	=	BloodGroup + 4*MedicalWarnings	
	DriverRecord	=	DriverID + LastStartTime + UsageCode	
	EngineManagementCriteria	=	MaxRevsAtThrottleSetting + MaxThrottleSettingAtRevs	20
	EngineNo	=	*(see VehicleDetails)*	20
	EngineRevs	=	*(see EngineSettings)*	2
	EngineSettings	=	EngineRevs + Temperature + OilPressure +IntakeManifoldPressure + ThrottleSetting	
	ExpiryDate	=	*(see LicenseDetails)*	6
	ExtAuthDetail	=	*a matrix 8 X 10 each 2 bytes (ExternalAuthCode by ResponseDefinition)*	
	ExternalAuthCode	=	*identifies external authority*	2
	ExternalAuthorityQuery	=	ExternalAuthCode + ExternalAuthQuery	
	ExternalAuthQuery	=	* Some vehicle details (FrameNo, EngineNo), some owner details, some driver details, some license details and some sensor readings*	
	FrameNo	=	*(see VehicleDetails)*	20
	IntakeManifoldPressure	=	*(see EngineSettings)*	10
	IssueAuthority	=	*(see LicenseDetails)*	10
	LastStartTime	=	*(see SensorReadings)*	10
	LicenseDataInAccordanceWith AppropriateDefinition	=	License data that owner has authorised for release to external authorities	
	LicenseDetails	=	LicenseNo + DOB + ExpiryDate + Category + Condition + IssueAuthority	
	LicenseNo	=	*(see LicenseDetails)*	10
	Make	=	*(see VehicleDetails)*	20
	MedicalWarning	=	*a code to identify allergies etc *	2
	MirrorSetting	=	*(see PersonalSettings)*	50
	Model	=	*(see VehicleDetails)*	20
	OilPressure	=	*(see SensorReadings)*	2
	OwnerAccess	=	OwnerID + OwnerEnrolAuthData	
	OwnerAuthSupplied	=	[PIN | TransponderSignal | BioTemplate]	8 - 256
	OwnerDetails	=	OwnerAccess + OwnerName	
	OwnerEnrolAuthData	=	[PIN | TransponderSignal | BioTemplate]	8 - 256
	OwnerID	=	*(see OwnerDetails)*	2

	OwnerName	=	*(see OwnerDetails)*	30
	OwnerQuery	=	OwnererID + OwnerAuthSupplied + DataRequired	
	Payment	=	*sum deducted from purse balance*	2
	PersonalisationData	=	EngineManagementCriteria + PersonalSettings	
	PersonalSettings	=	SeatSetting + MirrorSetting	
	PreviousMaxmia	=	*data items potentially updateable*	
	PreviousReadings	=	*data items potentially updateable*	
	PreviousReadTime	=	*data items potentially updateable*	
	PreviousSartTime	=	*data items potentially updateable*	
	Pulse	=	*an event initiated by the engine*	
	PurseBalance	=	*cash available to the driver*	10
	Readings	=	*updated previous readings*	
	Registration	=	*(see VehicleDetails)*	7
	ResponseDefinition	=	*defines what response may be made to an external enquiry*	
	ResponseToExtAuth	=	*Authorised data as specified*	
	ResponseToOwner	=	* Data as specified by the owner(Alias RequiredData)*	
	RoadUseDirections	=	*provided by external authority*	
	SeatSetting	=	*(see PersonalSettings)*	50
	SemsorReadingsAsAppropriate	=	*alias Readings*	
	SensorReadings	=	Acc/deceleration +EngineRevs + IntakeManifoldPressure +LastStartTime + Last30PeriodicReadingsSpeed + Last30PeriodicReadingsDeceleration + MaxDecelerationSinceLastRead + MaxOilPressureSinceLastRead + MaxPowerSinceLastRead + MaxRevolutionsSinceLastRead + MaxSpeedSinceLastRead + OdometerReading + SpeedKPH + Temperature + ThrottleSetting + TimeLastRead + Time (Date-time group) ActualPersonalSettings	
	Speed (Valet set)	=	*(see ValetOpConditions)*	2
	StorableReadings	=	*alias Readings*	
	Temperature	=	*(see EngineSettings)*	2
	ThrottleSetting	=	*(see EngineSettings)*	10
	TransactionAmount	=	*(see TransactionDetail)*	10
	TransactionDate	=	*(see TransactionDetail)*	6
	TransactionDetail	=	TransactionDate + TransactionAmount	
	UsageCode	=	*indicates purpose of journey*	2
	UseCode	=	*alias UsageCode*	
	ValetArming/DisarmingCode	=	*activates microcontrollers if ValetOpConditions are met*	
	ValetCodes	=	*codes potentially selectable by the owner*	
	ValetOpConditions	=	Date + Speed + Distance	
	ValetReset	=	*removes constraint imposed by ValetSet*	
	ValetSet	=	*causes the microcontrollers to enforce conformance to the ValetOpConditions*	
	ValetSetSupplied	=	[ValetReset | (ValetSet + ValetOpConditions)]	
	VehicleDetail	=	Make + Model + Registration + EngineNo + FrameNo + YearOfManufacture	
	YearOfManufacture	=	*(see VehicleDetails)*	2

Appendix 6

QUESTIONNAIRE

Fleet Operator:

A fleet manager needs data upon which to base his decisions.
The purpose of this questionnaire is to get your advice as to what data your organisatiuon collects, how it is collected, stored and retrieved, and whether, in your opinion, the process could be improved using modern technology.

1. What data is recorded:

   Usage: driver details?
   journey purpose?
   kms covered?
   defects observed?
   fuel etc. supplied?
   other?

   Maintenance
   routine checks?
   repairs?
   other?

There are several ways of collecting data:

A. By the driver, or other person, keeping a diary or log sheet manually with a pen/pencil
B. By a fuel station automatically reading the driver's fuel card and the pump dispensing meter. This is supplemented by the keyboard entry of the odometer reading as advised by the driver. These data are periodically passed to the fleet owner, either electronically or by a paper report.
C. By a repair or service workshop providing documents such as quotes and invoices whose details are entered into the fleet owner's database, either by filing the documents or by keyboard.
D. Other.

2. How is the data collected?

   Usage: driver details?
   journey purpose?
   kms covered?
   defects observed?
   fuel etc. supplied?
   other?

   Maintenance
   routine checks?
   repairs?
   other?

Data can also be stored in different ways.

A. *In paper files?*
B. *Digitally? (e.g. in a database)*
C. *Other.*

3. How is the data stored:

   Usage: driver details?
   journey purpose?
   kms covered?
   defects observed?
   fuel etc. supplied?
   other?

   Maintenance
   routine checks?
   repairs?
   other?

4. Do you feel your current system is satisfactory or do you have eventual changes in mind?

5. Do you feel users and others co-operate satisfactorily?

6. Assuming the price was right , would you consider a system that automated most data collection?

7. If not, what would be your objection?

8. If so, what do you think would be an acceptable price for the in-vehicle unit of an automatic system?

Appendix 7

PASCAL CODE TO MANIPULATE SMARTCARD READER

```
(* This program accesses SCOS based on the Intel 8051 chip in the
smartcard reader, reads a codeword from a smartcard via ComPort2, and
passes it to ComPort1 for reception by the HC11 microcontroller. In
doing so it simulates a more sophisticated reader *)

Program PassCode;

uses
  CRT,        {Standard Turbo Pascal unit}
  Misc,       {Standard Turbo Pascal unit}
  IO,         {Unit obtained from Chris Barrett}
  SCOS,       {Unit obtained from Chris Barrett}
  CtrlCmds,   {Unit obtained from Chris Barrett}
  ASYNC;      {Unit obtained from Rising Edge Technology}

const
  ComPort1 = 1;  {The port used to communicate with the HC11}
  ComPort2 = 2;  {The port used to communicate with the reader}

var
  SaveExit : pointer;
  Status : integer;
  StatusStr : String;
  BufStr : String;
  Buffer : BufType; {Type defined in unit IO}
  I      : Byte;

{---------------------------------------------------------------------}

procedure CloseDown; Far;

begin
  WriteLn ('Now in Closedown  ');
  ExitProc := SaveExit;
  { Attempt to close down the Communications Port (IO.PAS 4)}

  If CloseCommPort(ComPort2) then
    Writeln('COM',ComPort2,' closed successfully!')
  else
    begin
      Writeln('Unable to close COM',ComPort2);
      Halt;
    end;

  If CloseCommPort(ComPort1) then
    Writeln('COM',ComPort1,' closed successfully!')
  else
    begin
      Writeln('Unable to close COM',ComPort1);
      Exit;
    end;
  end;  {CloseDown}

  {------------------------------------------------------------------}
  procedure SendArmingCode;

  begin  {SendArmingCode}

    {Install exit procedure to close down the communication port}
    SaveExit := ExitProc;
    ExitProc := @Closedown;

    { Attempt to open the Communications Port (IO.PAS 3)}

    If OpenCommPort(ComPort1) then
           Writeln('COM',ComPort1,' opened successfully!')
    else
      begin
        Writeln('Unable to open COM',ComPort1);
        Halt;
      end;

  writeln ('Ready to write CODEWORD to ComPort 1');
  ComWrite (ComPort1, BufStr);      {ASYNC19 writes BufStr to
Comport1}
  writeln ('Codeword sent');
  readln;

  end;  {SendArmingCode}

  {---------------------------------------------------------------}

begin  {PassCode main program}
  ClrScr;

  if not Initialise_SCAM(ComPort2) then  { Uses unit CtrlCmds }
    begin
      WriteLn('SCAM Initialisation Error');
      halt;
    end;
  readln;

  if not Initialise_SCOS then           { Uses unit Scos }
    begin
      WriteLn('SCOS Initialisation Error');
      halt;
    end;
  readln;

  Write('Select Directory #4 - ');  (* Selects card directory
                                       containing codeword *)
  Status := Sel_Dir(4);
  SCOS_Error(Status,StatusStr);
  WriteLn(StatusStr);
  readln;

  Write('Open File #1 - ');         (* Opens the card file
                                       containing codeword *)
  Status := Open_File(1);
  SCOS_Error(Status,StatusStr);
  WriteLn(StatusStr);
  readln;

  if Status = File_Not_Found then
      Writeln('File not found. Must create File  ');
  Write('Read File #1 (RecNum = 1, Len = 8) - ');
                                     (* Reads the codeword
                                        from the card *)
  Status := Read_File(1,8,Buffer);
  SCOS_Error(Status,StatusStr);
  WriteLn(StatusStr);
  readln;

  Move(Buffer,BufStr[1],8);
  BufStr[0] := #8;
  WriteLn('BufStr = ',BufStr);

  SendArmingCode;
  writeln('SendArmingCode exited');
  readln;
end.
```

Appendix 8

MICROCONTROLLER CODE FOR HC11

```
0001    0000            ;
0002    0000            ;
0003    0000
0004    0000
0005    0000
;*****************************************************************
0006    0000            ;  A program to pass a codeword to the HC11
                        ; microcontroller, compare it
0007    0000            ;  to the codeword already stored in RAM in
                        ; the microcontroller and,
0008    0000            ;  if the two are the same, output a small
                        ; current and voltage to
0009    0000            ;  switch  on a thyristor.
0010    0000            ;                             by
0011    0000            ;                          Harry Jones
0012    0000            ;              File: ARMCARV.ASM  version for RAM
0013    0000            ;                         19th  JULY, 1998
0014    0000            ;           assemble with tasm using tasm11s.bat
0015    0000
;*********************************************************************
0016    0000
0017    0000
;*********************************************************************
0018    0000
0019    0000            ;                        EQUATE TABLE
0020    0000
0021    0000            ; addresses
0022    0000
0023    0000            ADDRESS  .EQU   $D000    ;Supplied code stored
                                                 ;here
0024    0000            CODESPOT .EQU   $B700    ;On-board code stored
                                                 ;here
0025    0000            REGBASE  .EQU   $1000    ;Register base address
0026    0000
0027    0000                                     ; parameters
0028    0000
0029    0000            BAUDDAT  .EQU   $30      ;Sets baud rate
0030    0000            CONF1    .EQU   $00      ;Configures frame
0031    0000            CONF2    .EQU   $0C      ;Enables transmit
                                                 ;&receive
0032    0000            SELPIN   .EQU   $20      ;Select Port pin
0033    0000
0034    0000            ; offsets
0035    0000
0036    0000            BAUD     .EQU   $2B      ;Baud register offset
0037    0000            DATA     .EQU   $2F      ;Data register offset
0038    0000            DDRD     .EQU   $09      ;Port D data direction
                                                 ;reg
0039    0000            NUMCHAR  .EQU   $08      ;Number of chars in
                                                 ;CODEWORD
0040    0000            NUMFLASH .EQU   $20      ;Twice number of
                                                 ;flashes
0041    0000            PORTD    .EQU   $08      ;Port D offset
0042    0000            SCCR1    .EQU   $2C      ;SCI con reg 1 offset
0043    0000            SCCR2    .EQU   $2D      ;SCI con reg 2 offset
0044    0000            STATUS   .EQU   $2E      ;SCI status register
```

```
;                                          ;offset
0000
0000            ;************RECEIVE SUPPLIED CODEWORD ******
0000            ; This program will receive characters from
0000            ;the PC if it is installed in RAM on the hc11
                 ;microcontroller and the command GO c000 is
0000            :;issued
0000     ;*************************************************
0000

B600                       .org   $B600   ; For EEPROM use B600
B600
B600      ;************PREPARE TO RECEIVE CODEWORD***********
B600      ; Set up the parameters for Serial Communication
B600      ; Interface reception.
B600      ;**********************************************
B600
B600 CE 10 00  START:  ldx   #REGBASE ; Sets index to regstr
                                         ;base.
B603 1C 08 20          bset  PORTD,x,SELPIN ;Ensures pin
B606                                    ;D5 set on start.
                                         ;Inverter acts on it.
B606 86 30             ldaa  #BAUDDAT ; (sets baud to 9600 by
B608 A7 2B             staa  BAUD,x   ; setting bits SCP1 SCP0)
B60A                            ; (bits 4 & 5 in baud register)
B60A 86 00             ldaa  #CONF1   ;(1 start bit, 8 data
B60C A7 2C             staa  SCCR1,x  ; bits & 1 stop bit)
B60E 86 0C             ldaa  #CONF2   ;(transmit & receive
                                      ; enables TE = RE = 1 in
B610 A7 2D             staa  SCCR2,x  ; SCCR2)
B612                               ;(bits 2 & 3 are set by $0C)
B612 86 20             ldaa  #SELPIN  ;(Sets data direction
                                      ; for Port D5 to become
B614 A7 09             staa  DDRD,x   ; output for LED &
B616                                           ; thyristor)
B616 18 CE D0 00       ldy   #ADDRESS ;Store received data here
B61A
B61A   ;************RECEIVE CODEWORD CHARACTERS**************
B61A   ; The program will cycle at this point until a character
B61A            ; is received.
B61A   ;************************************************
B61A A6 2E   RECVCHAR: ldaa  STATUS,x ; (Proceed if RDRF = 1
B61C 84 20             anda  #SELPIN  ; (Anding with $20
                                         ;results in $00
B61E                                  ;  if RDRF bit is not
                                         ;set. It will be set
B61E                                 ; when data arrives & show
B61E                                    ;receive data reg full.
B61E 27 FA             beq   RECVCHAR ;  If so, loop)
B620 A6 2E             ldaa  STATUS,x ; (Read SCSR & data char
B622 A6 2F             ldaa  DATA,x   ;  and so clear RDRF)
B624                                  ; Para 5-9 of HC11 manual
B624 18 A7 00          staa  0,y      ; Store char at ADDRESS.
B627 18 08             iny              ; (Inc index until all
B629 18 8C D0 08       cpy   #$d008   ;  chars (8) received)
B62D 26 EB             bne   RECVCHAR ; Get next char
B62F
B62F     ;*********COMPARE STORED TO SUPPLIED CODEWORD*******
B62F       NOTE: BUFFALO Memory Modify HAS BEEN used to put the
B62F      ; stored code at  CODESPOT IN E2PROM. If the supplied
B62F            ; code matches the stored code an LED flashes
B62F        ; as a visual signal and 5V is supplied to pin PD5.
```

```
B62F      ;****************************************************
B62F
B62F CE B7 00         ldx   #CODESPOT    ; Stored CODEWORD here
B632 18 CE D0 00      ldy   #ADDRESS     ; Reset y to addr
B636 C6 08            ldab  #NUMCHAR      ; CODEWORD is 8 chars
B638 18 A6 00  LOOP1: ldaa  $00,y         ; Acc loaded with
B63B                                   ; suppld char from ADDRESS
B63B A1 00            cmpa  $00,x         ; Compares to stored
B63D                                      ; char from CODESPOT
B63D 26 16            bne   RESTORE       ; If no match then
B63F                                   ; error RESTORE resets all
B63F                                 ; values and then returns to
B63F                                  ; the waiting loop RECVCHAR.
B63F 08               inx
B640 18 08            iny
B642 5A               decb               ; Set-up for next char
B643 26 F3            bne   LOOP1         ; Loop for 8 chars
B645
B645      ;*************OPEN GATE & FLASH LED *****************
B645      ; Routine puts eight pulses on Port D5. This activates
B645      ; the thyrister gate and causes the LED to flash on
B645      ; sixteen times.
B645      ;***************************************************
B645
B645 CE 10 00         ldx   #REGBASE ; restored from CODESPOT
B648 C6 20            ldab  #NUMFLASH ;Number of LED changes.
B64A                      ;Flashes half the number of changes.
B64A 86 20            ldaa  #SELPIN  ; Selects bit 5
B64C 88 20    LOOP3:  eora  #SELPIN  ; Self XOR toggles bit 5
                                              ;on/off
B64E A7 08            staa  PORTD,x  ; Activates/Deactivates D5
B650 8D 20            bsr   DELAY    ; enables LED to be seen
B652 5A               decb           ; after 16 flashes = 0
B653 26 F7            bne   LOOP3    ; repeat until count is 0
B655                                 ; return to loop waiting
B655                                 ; for CODEWORD
B655
B655      ;*********PREPARE TO RETURN TO WAIT LOOP*************
B655        ; routine to restore loop waiting for supplied code
B655      ;****************************************************
B655 CE 10 00  RESTORE:  ldx #REGBASE    ; Only needed in
                                              ;restoring from ERROR
B658                                 ; (Restored from CODESPOT)
B658 18 CE D0 00     ldy  #ADDRESS  ; location of supplied code
B65C                           ; (Restored after DELAY routine)
B65C 86 FF     NEXT: ldaa #$ff     ; Overwrites a supplied code
B65E 18 A7 00        staa 0,y         ; character with ff
B661 18 08           iny            ; Then next code character
B663 18 8C D0 08     cpy  #$d008      ; until 8 chars.
B667 26 F3           bne  NEXT        ; Overwrite next char
B669 1C 08 20        bset PORTD,x,SELPIN ;Ensures pin D5 set ON
B66C                      ; at each RESTORE. Inverter acts to
B66C                          ; make it OFF until ON in LOOP 3.
B66C 18 CE D0 00     ldy  #ADDRESS    ; After 8 chars reset the
                                              ;index &
B670 20 A8           bra  RECVCHAR    ; return to wait loop
B672
B672      ;***************DELAY*******************************
B672      ; a delay routine to enable flashes to be seen
B672      ;****************************************************
B672 18 3C       DELAY:      pshy
```

```
0156   B674 18 CE FF FF            ldy      #$FFFF ; Contaminates Y
0157   B678 18 09       LOOP2:     dey
0158   B67A 26 FC                  bne      LOOP2
0159   B67C 18 38                  puly
0160   B67E 39                     rts
0161   B67F
0162   B67F
0163   B67F                     .end
tasm: Number of errors = 0
```

Appendix 9

VEHICLE SECURITY SURVEY

Reg No

No pen needed. Just prick six holes and drop it.

QUESTIONS

The following five questions are intended to get your opinion as to what a motorist might pay for security. Some reasons why you might respond ——→

Ultimate security that would defeat almost any thief can be installed on almost any vehicle. For details——→

Q1 What would you be prepared to pay for *ultimate* security?

more|$500|$100|$50|$25|$10|less

(Prick your choice with the toothpick)

Pretty good security that would defeat most joyriders and impulse thieves is installed on some modern vehicles. For details ——→

Q2 What would you be prepared to pay for *pretty good* security?

more|$500|$100|$50|$25|$10|less

(Prick your choice with the toothpick)

Standard security is fitted to most older vehicles. ——→

Q3 Do you think this is enough?

yes / no

(Prick your choice with the toothpick)

Q4 Do you think alarms or immobilisers are worth fitting?

yes / no

(Prick your choice with the toothpick)

Q5 If YES, how much would you be prepared to pay for one?

more|$500|$100|$50|$25|$10|less

(Prick your choice with the toothpick)

FURTHER INFORMATION FOR THOSE INTERESTED

In Western Australia almost 20,000 vehicles are stolen every year and the number is rising. You can help to change that. For most people a car is their second most valuable asset and it is the easiest to steal. Your answer, by indicating just five choices, will help a study of the options for making vehicle theft harder. Security is often defined as the preservation of one's assets. Therefore, the cost of security must be balanced against the possibility of loss. The purpose of this questionnaire is to get your views on what kind of balance motorists might choose.

The *ultimate* vehicle security system is one that requires the presentation by the legitimate driver of a personal feature such as a fingerprint, eye retina or back-of-hand for scanning. Only when the presented feature matches its description stored in the vehicle will the doors, bonnet and boot open, ignition and fuel systems work and steering, brakes and gearbox be released. Also, if the engine is switched off and no one is in the vehicle, then after a short period the doors will be locked and the other systems deactivated

A *pretty good vehicle security* system is one that requires the presentation of a device that responds to a radio challenge from the vehicle with a code that causes the vehicle doors to open and, on entry of a PIN using a keypad within the vehicle, enables the ignition and bonnet catch to work and unlocks the steering. The device presented is no bigger than a key tag.

A *standard* security system is one that requires a key to unlock the doors, bonnet and steering and activate the ignition.

Do you have any suggestions or comments?

....

....

....

....

WHAT TO DO WITH COMPLETED QUESTIONNAIRE

Drop it on the ground for later collection. (the weight will prevent it blowing away) or

put it in any of the boxes at the exits from the car park, or

drop it in the Building 13, Computer Science assignment box, or

give it to the Secretary, Computer Science Department

Appendix 10

LIST OF ACRONYMS

ABA	American Bankering Assoc
ABS	Acrylonitrile Butadiene Styrene
ADEPT	Automatic Debiting and Electronic Payment for Transport
API	Application Programming Interface
ARM	Advanced RISC Machines
ATM	Automatic teller machine
BAPI	Biometrics API
CASCADE	Chip Architecture for SmartCArds and secure portable DEvices
CCD	Charge Coupled Device
CCITT	Comite Consultatif International de Telegraphic et Telephonic
CCT	Card Technology Today
CCTA	Central Computer & Telecommunications Agency
CD/ROM	Compact disk / read only memory
CEN	Comite Europeen de Normalisation
CEO	Chief executive officer
CEPS	Common electronic purse specification
CLIP	Classical Internet Prorocal (over ATM)
CLIP	an electronic purse system
CMOS	Compatible metal oxide semiconductor
DES	Data Encryption Standard
ECU	Edith Cowan University
EEPROM	electronically erasable programmable ROM
EFTPOS	Electronic funds transfer point of sale
EMV	Europay Mastercard Visa
EPROM	electrically programmable ROM
ESPRIT	European Strategy for Promotion of Research in Information Technology
ETSI	European Telecommunications Standards Institute
Europay	Mastercard and Visa (EMV)
FAR	False Acceptance Rate
FeRAM	Ferroelectric RAM
FRR	False rejection rate
GDP	WA's Gross Domestic Product
GDP	Gross domestic product
GPS	Global Positioning Systems
GSM	Global System for Mobile communication
HBF	Health Benefit Fund
IBIA	International Biometric Industry Association
IC	Integrated circuit
ICSA	International Computer Security Association
ID	Identification

INRIA	Institute for Research in Automation
ISO	International standards Organisation
IVHS	Intelligent vehicle highway system
K	kilo or 1024 bytes
LWB	Long Wheel Base
MCU	Microcontroller
MHz	megahertz
MIFARE	An industry standard contactless card operating system
MTL	Mount Lawley
MULTOS	Multi-application Operating System
NEC	Nippon Electronic Corporation
NRI	National Registry Inc
NZ	New Zealand
OBD	on-board diagnostic
OBD	On-board diagnostics
OMI	Open Microprocessor Initiative
PACT	Partners Against Car Theft
PC	Personal computer
PC/SC	Personal computer / smartcard – a protocol
PIN	Personal identification number
PKI	Public Key Certification infrastructure
PVC	Polyvinyl Chloride
RAC	The Royal Automobile Club of WA or UK
RAM	random access memory
RISC	Reduced Instruction Set Computing
ROC	Receiver operating curves
ROM	read only memory
RSA	Rivest Shamir Adelmann - an assymetric cryptography method
SA	South Australia
SAM	smartcard access module.
SCALPS	smartcard chip for limited payment systems.
SET	Secure electronic protocol
SIM	Subscriber Identity Module
SJB	?
SNCF	Societe Nationale des Chemins de Fer Francais
SSS	Smart Silicon Systems Ltd
UK	United Kingdom
US	United States
USA	United states of America
UWA	University of WA
VATS	Vehicle Anti-theft System
VP	Vice President
WA	Western Australia
WWW	World wide web