

U-notat 5/2002

Virtual keys – the Janus face of ICT?

Helge Godoe

Contents

1	The rationale for exploring and analyzing ICT keys.....	5
	Introduction: Explaining design and construction of ICT	5
	The significance of virtual keys	5
	Exploring virtual keys – how the inquiry evolved.....	8
	Approaching virtual keys as smart cards	10
	The Web as a source	10
	Making observations of the smart card community.....	12
	Plan of this report.....	16
2	Theories explaining construction technology and ICT.....	18
	Introduction: Explaining ICT construction as virtual keys.....	18
	Technological construction in the ICT sector: The landscape, facts and taxonomical approach.....	18
	Mainstream explanations of technological construction.....	22
	Optimization theories.....	25
	Social constructionist theories	28
	Discussion	31
3	Smart cards - the Janus of ICT?	33
	Smart card technology	36
	A brief history of smart cards	42
4	Continuity and discontinuity in locks and keys	46
	Introduction: How novel are innovations?.....	46
	A brief history of keys	51
	Mechanical locks	54
	Information-based locks.....	57
	Cryptography	59
	Lock-picking and cryptoanalysis	62
	Discussion – continuity and discontinuity?	66
5	Diffusion of smart card technology	68
	Empirical approach	72
	Development and diffusion projects	73
	The rationale for smart cards	74
	Financial service cluster.....	74
	Telecom service cluster.....	75
	Organizational process reengineering cluster	76
	Smart card technology suppliers.....	78
	A common understanding of smart card technology	79

Physical cash vs. electronic cash	79
The trust factor	80
Biometric keys	81
Smart card technology standards	81
Multi-application smart cards	82
Technological systems, competition and diffusion.....	83
6 Electronic money and smart cards.....	87
Introduction: The problem of electronic money	87
Cash and electronic payment in Norway	88
The persistence of physical cash.....	91
The nature of money	92
The idea of money	93
The role of money in society	95
Discussion: Money and smart cards	97
7 Conclusion: Explaining virtual keys	101
The shift in focus and increased complexity.....	101
SIM-cards and other smart cards	102
Virtual keys and current theories explaining technology	105
The impact of virtual keys	107
Literature.....	109

1 The rationale for exploring and analyzing ICT keys

Introduction: Explaining design and construction of ICT

This report attempts to explore new ways of explaining how technology, in particular information and communication technology (ICT), is developed. This is an immense subject; for this reason a compromise has been made in terms of delimitation and focus: The main topic of this report will be the new, ICT-based *virtual keys*. In brief, the virtual keys are ICT-based regulation technologies, such as embodied in smart cards, PIN-codes, biometric keys, cryptographic algorithms, magnetic stripe cards, etc. These technologies have primarily been created and designed in order to control, or regulate, the use of ICT; a virtual key will give users access to an ICT-system and its applications, as evident when a person inserts his or her plastic card in an ATM and enters a PIN-code. Broadly following the logic and procedures of a case-study approach, cf. (Yin 1989), the choice of virtual keys as the object of study and analysis is not arbitrary, it is *strategic*: On the one side, the development of virtual keys is typical of technological construction, design and development; the virtual keys mirror ICT development and diffusion as a technological *project*. On the other side, the virtual keys are social technologies. Mechanical and information based keys and locks have been in use in societies for thousand of years for social reasons, i.e. to regulate (secure, control, immobilize, keep secret, manage, prevent burglary, etc) whatever various groups and individuals consider valuable or vulnerable. Thus, one may analyze and discuss to what extent the virtual keys are really novel, because many aspects of these bear strong resemblance to antecedents that have existed for a long time prior to the emergence of ICT. This, in turn, may elucidate to what extent ICT has novel social and cultural aspects, i.e. the impact of what designers of technology create and how users, markets and social systems respond to and influence the shaping and design of the virtual keys. In this, an analysis of the diffusion of virtual keys is interesting because this will provide insights into these aspects. For this reason, focus will be set on the design, construction and diffusion of smart cards.

The significance of virtual keys

The selection of ICT keys as an object or case for analysis is *strategic* because of the advantages this will provide for explaining how and why ICT develops, i.e. this was chosen for a number of specific reasons. First of all, because of the magnitude and enormity of explaining ICT construction, design and diffusion there was the need to delimit the size of this inquiry, specifically in order to focus. Secondly, because of the first consideration, the object of analysis should significantly reflect important issues related to ICT and its development. Simultaneously, this should reflect non-trivial factors in the role of ICT in modern, contemporary societies and cultures – and to what extent these aspects are related to or

interact with design, construction and diffusion of ICT. Finally, the inquiry should provide empirical insights elucidating to what extent this represents something new, compared with “pre-ICT” technological design, construction and diffusion. Thus, in selecting ICT keys these general criteria served as a filter that eliminated other possible objects of inquiry. In addition to these, there are numerous aspects related to ICT keys which made them attractive as objects of inquiry and analysis, i.e. why selection of this is strategic:

- *Communication and interaction* in society is increasingly regulated by ICT-based keys; without possession of these keys, restraints and disabilities are imposed on individuals in terms of interaction, expression and movement, as evident in the notion of an emerging *digital divide* in society, i.e. the social differentiation (possibly, discrimination) created by the immersion of ICT in society. The immediate reason for this is that ICT-based keys are increasingly used for access control, usually by means of magnetic stripe cards or smart cards, in combination with passwords. These keys give access to important societal assets, material or non-material, such as buildings, banking accounts, computer systems, mobile telephones, etc. The implications of this are complex, in particular related to various considerations in terms of security and privacy issues. Still, ICT-based keys are characterized by their dual nature: Whereas these keys may potentially increase regulation and control, i.e. restriction of freedom and privacy, they are also capable of providing systems with more flexibility and delegation of freedom to its users. Many appreciate the latter; they cherish anonymity - less social control and its associated hassle and nosiness gives a feeling of freedom.
- *Capability of articulation* has increased dramatically in the ICT-based keys, compared to mechanical key, primarily in terms of volume, memory, processing capability and programmability. This, in turn, has increased the versatility of these keys; because of the keys' programmability, designers of keys may be able to insert numerous instructions as to how people should act – to users this may represent new potentials and opportunities.
- *Control of morality and behavior* may be embodied in the design of ICT-keys to an extent and degree that was neither possible with mechanical keys, nor with equivalent systems run by human beings. The most obvious aspect of this is the phenomenon of electronic traces – and how people, because they have knowledge of this, adjust their behavior to this: People know that the keys will leave telltale evidence of what they have done or neglected – that the system may betray them and that the burden of proof now will rest with them.
- *Money and valuables* are increasingly articulated as information in ICT-systems, these in turn being controlled by ICT-based keys. Simultaneously, the increased capability of articulation enables a type of precision that was impractical in the pre-ICT age, as evident in the currency exchange rates that are now quoted with decimals that do not exist in physical cash, e.g. that the Euro is exchanged with US\$ at the rate of 0,9783. As a normal user, this makes it possible to become more mobile – a small plastic card will enable a person to travel to the other side of the globe and, by inserting the card into an ATM and entering the PIN-code, get this machine to spew out cash within seconds and without talking to anyone.

- *Privacy and confidentiality* is to an increasing extent managed by ICT-based keys, however, these aspects also create problems and conflicts in relationship to ownership of information. A related conflict may be observed in the disputes over IPR, intellectual property rights, as evident in controversies about music distributed on the internet (e.g. Napster) and the attempts by entertainment industry to insert various ICT-based locks into CDs in order to prevent what they consider misuse, i.e. illegal copying or “piracy”. Governments and their security agencies have expressed concern and tried to prevent the commercial diffusion of cryptography, as evident in the conflicts between mobile telecommunications operators and police on who should pay for the expensive equipment needed for eavesdropping on GSM. Those who designed GSM made a complex signal code for this system, because the old mobile systems were notorious for their lack of privacy.
- *Freedom of expression and the free flow of information* are aspects that confront the diffusion of ICT-based keys; as these are used increasingly, they create tension and conflict for some, while for others this represents exciting prospects and opportunities: ICT-keys may be designed to function as information and communication filters, such as “porn-filters” in TV-sets and on the internet¹. As a filter, the ICT-keys restrict the free flow of information – those who control the keys decide what may be communicated or distributed. Some may consider this discrimination and censorship, i.e. anti-democratic and authoritarian, while others will defend this as legitimate: Every individual has a right to protect his own sense of integrity; every nation, society or family has a legitimate right to put a taboo on information they consider immoral or dangerous, as evident in Singapore, in the governments policy of censorship of the Internet. ICT-keys are also used commercially, especially in distribution of pay-TV and these may be tailored in numerous ways. As the various medias are converging, specifically as the distinction between one-way and two-way communication is diluted, the issue of controlling ICT-keys may increasingly become a question of freedom of expression and flow of information and communication.
- *Public and national interests* are involved in the design and dissemination of ICT-based keys, in a multitude of dimensions, as evident in the struggle for who should have the ultimate hegemony over cryptography. A related aspect is the phenomenon of hacking and “data virus”: An aspect of hacking is the skills involved in picking various ICT-based locking mechanisms and the creation of computer programs that instruct the computers connected to networks to do strange things, i.e. the creation of “data virus”.
- *Identities in cyber culture* are increasingly influenced by the interaction and experience people have with ICT and their encounters with ICT-keys. As a result, this familiarity

¹ Cf. <http://www.getnetwise.org/tools/filters.php> - at this site on the web, advice is given on various types of filters. Under the headlines “Tools for Families” and “Tools that block access to content”, an introduction to the topic states that: “If you are concerned that your child may be reading or viewing material online that you consider inappropriate or harmful, you may want to think about filtering tools. There are a lot of filtering tools, and they do not all work the same way.” Below this, a list of various types of filters are described and offered for sale.

make people attribute anthropomorphic traits to ICT, as evident in a typical everyday statement that “the ATM *ate* my bank card because I *pressed* the wrong code”, or attributing a gender to the PC or mobile telephone, akin to what sailors do when they think and speak of ships as females.

Exploring virtual keys – how the inquiry evolved

In planning the inquiry on virtual keys, the initial idea was that a detailed laboratory study of how these are developed would provide the needed empirical data. As a first step, during the autumn of 1998 and early 1999, I completed an initial survey which included visits to a number of R&D departments in eight companies in Norway, interviewing representatives of these. Seven of these were typical of ICT firms in the virtual keys business – the eighth was a traditional company manufacturing mechanical locks and keys. The idea of including the latter in the study was to have a case for comparing construction and design of ICT based keys with non-ICT keys and locks. In the course of this, I discovered that the real issues with developing, designing and constructing virtual keys are not so much within the laboratories as outside the companies, i.e. the critical “design-parameters” evolve outside the laboratory and the firm. The work undertaken and classified as R&D in the companies, however ingenious, are mostly related to incremental software engineering and affiliated system integration, in product development. This is undertaken by adapting fairly standardized solutions to various applications. As one of the R&D-managers explained to me: “The technology we use is “commodities”² – we buy this off the shelf from whoever sells this at the lowest price”. Others explained that, in addition, it is important for their business and R&D to participate on the international scene, because this is where important decisions are made, i.e. they work in a market environment ruled by international technological diplomacy and power-struggle.

Parallel to this, I was pursuing a related line of inquiry that led me into the phenomenon of computer hacking. In the long history of mechanical and information-based keys and locks, there is a parallel history – at most times highly secret and illegal – of those who pick keys. In order to understand virtual keys, a closer look at computer hacking would be advantageous. Based on some previous knowledge of the computer hacker community in Norway, I undertook a broad survey of the literature on hacking, mainly on the Web, in addition to closer analysis of some recent “hacker incidents” reported in the media. Although the results of this study has been published elsewhere, (cf. Godø 1999; Godø 2002) – it became clear that this phenomenon also has salient political aspects, because hacking may indeed be interpreted as a proto-political movement based on strong ideals as to how ICT should evolve.

The result of this study of hackers’ role in virtual keys and the initial survey of R&D in companies constructing and designing virtual keys led to a shift of attention, a shift away

² In industrial jargon, “commodity” means a standardized, mass-produced, usually inexpensive product or component.

from the lab towards a more diffuse arena: The dynamics and actors trying to promote virtual keys as systems and their environment. By this, the notion of the lab that designs and constructs virtual keys was transformed to a system of interrelated actors, sometimes highly organized – at other times anarchistic or strongly competitive. In this, the smart card industry emerged as a significant player, however, this being closely tied to (or subordinate, some would even claim) to strong institutional actors found in the ICT-industry in general (in particular, the telecommunication industry) and in banking (electronic payment), governments, etc. The picture that gradually emerged was that in the development and diffusion of virtual keys, the technology (hardware, etc.) had become stabilized; there is indeed a *dominant design* (Abernathy and Clark 1985; Utterbach and Suarez 1993), as evident in the ISO 8716 standard for smart cards or the GSM 11.11 standard for SIM-cards, etc. The technology of virtual keys has increasingly become commodities, which may explain why some senior executives of smart card companies characterize their industry as "mature". This is not unique to the construction and design of virtual keys; this reflects a general tendency in engineering design, as observed by analysts of modern design and construction (cf. McAloone and Robotham 1999, p. 95-99): There is a general trend towards standardized technology "platforms" and modules; engineering design is increasingly a task of composing solutions based on these. The use of ICT (e.g.: CAD, simulation, rapid prototyping, advanced visualization, combinatorial design, etc.) has also changed the nature of work in designing and constructing new technology – more effort is put into the initial product and service concept development, the "packaging" of the product (aesthetics and styling) and market considerations, partly because of the automation and standardization of the technology. Recognizing and finally admitting this demanded a shift in the inquiry – a new exploration, i.e. an adjusted data collection strategy was devised in the spring of 2001:

- Selection of smart cards as the main object of inquiry in terms of virtual keys, posing the question of why smart card technology has succeeded in some areas (SIM-cards in the GSM mobile communication system), while the diffusion rate has been slow in other areas, even in France.
- Collection and analysis of literature on smart cards, in particular as this is presented on the Web.
- An in-depth inquiry into questions related to multiple uses of smart cards, i.e. what the industry calls "multi-applications", in particular its role as *electronic money*. This was considered strategic because of money's critical and pervasive role in society.
- Understanding how the actors in the smart card community (industry, government, R&D) think about and explain the development and future of smart cards. Data collection on this was undertaken by the following steps:
 - Observations at the Cartes 2001 in Paris, in October 2001,
 - Observations at the eEurope Smart Card Charter meeting at ETSI in December 2001,
 - In-depth interviews with seventeen project leaders responsible for large-scale smart card projects in Norway, during the spring of 2002.

Approaching virtual keys as smart cards

The selection of virtual keys as a topic was an attempt at delimiting the inquiry of how ICT is designed and constructed – and why this is undertaken. However, trying to understand and gather empirical material on virtual keys, outside the laboratory, in the “wilderness”, was much more difficult and complex than anticipated initially. Approaching the topic of virtual keys as an outside observer may resemble that of a diver who swims around a coral reef, making observations in an attempt to gather empirical data in order to understand and explain this universe: Everywhere, there are all kind of strange fish, strange in terms of color, shapes, the way they behave, etc. Some fish swim in schools in tight formation, others chase each other, still others seem to be in motionless meditation, some hide and dart away if other fish come too close, etc. Attempting to touch a fish is useless, it will immediately escape – using a spear for this will kill the fish. The coral reef in itself with its complex shapes and labyrinth-like structure and the way these reflect light create an environment for the fish which are difficult to comprehend: No apparent logic of landscape, always structural surprises – but still an environment which the fish apparently are comfortable with, they thrive here and nowhere else. Because of my experience with coral reef diving, I would claim observing the ICT industry and associated communities and markets for collecting data relevant for understanding and explaining the phenomenon of virtual keys is much more difficult and demanding.

The Web as a source

Just as with coral reef diving, one important reason for the difficulties encountered was, paradoxically, the wealth of information related to technological and market issues involving technologies that are used for the virtual keys, especially on the Web. The sheer volume of this type of literature and information was overwhelming. An indication of this may be found in the number of “hits” reported by search engines on the Internet: Typing “smart cards” (in two words) as a key word in the Google search engine yielded “ca. 1,4 million”³ hits as a result, i.e. the search engine had found 1,4 million documents on the Web in which “smart cards” were mentioned in some way or other. Entering the same key word in the AltaVista search engine gave the following response: “Refine your search with AltaVista Prisma”, this being accompanied by twelve subcategories related to smart cards. One of these, smart card solutions, had 6 856 links to URLs. As a paradoxical contrast, in using more academic search engines, such as the Bibsys, the national electronic library catalogue of universities and colleges in Norway, which is connected to equivalent international systems such as the ISI, this yielded almost no hits. Even if the key word “electronic money” did yield some more references, the results were meager. Thus, apart from one research institute⁴ that had some

³ The exact figure given was 1 430 000 in a search undertaken on 15th August 2002.

⁴ This was the Institute for Prospective Technological Studies, which is associated with the EU Joint Research Centre, located in Seville in Spain.

research activities related to virtual keys (electronic payment services and security issues), there was little relevant academic literature to guide and inform the inquiry.

The avalanche of URLs on the Web generated by the search engines when using the key word "smart cards" are, to the extent this has been surveyed⁵, industry-related technical and commercial information of all kinds, such as press releases, product information, company news, software information, etc. Of course, this has been an important and significant source of empirical data for the inquiry, specifically aspects related to technical and commercial factors, however, it has also created challenges. Primarily, its overwhelming volume, which makes it physically and economically impossible to get an oversight and equally difficult to keep pace with new developments, updates, etc. This task was sysophosic and at times frustrating, e.g. just trying to understand and assess the information in one interesting and relevant document found on the Web may lead to a whole day's work, because the document may have numerous links to other documents and Web-sites, if such leads were followed, then this in turn would give leads to still other sources of information, these too having appearances of being interesting and relevant for the research topic. Of course, sometimes the information found was difficult to understand because it was technically unfamiliar or incomprehensible, i.e. this was targeted to specialists and experts, such as numerous documents (proceedings, specifications, minutes of meetings, etc) from standardization bodies.

In spite of this overwhelming flood of information, the Web has been an important source in a number of ways: First of all, the sheer volume, its topics, style and rhetoric was information in itself, because this reflected the agendas and discourse culture of the players in the markets and industry. Secondly, even if highly technical information at times would seem inaccessible, this, more often than not, was more apparent than real: With some patience, even decoding and understanding details of JavaCard application software for smart cards or finer points in the structure and functioning of electric circuitry of the microprocessors in a smart card, was not unattainable, however, initially time consuming. Thirdly, a substantial share of the information on the Web and elsewhere is easy to comprehend; usually it is written in the clear and coherent prose typical of engineering communities, often generously illustrated with various graphics. The predominant language is English; apparently, even the large French smart card industry use English much.⁶ Thus, the sheer volume of information proved to be a formidable challenge in terms of being a source of empirical data. In this, making selections and interpretations of course became difficult.

⁵ At one point in the summer of 2001, I printed out and scrutinized the first 100 (approximately) URL-titles from a Google search. This took almost one week of work. Looking at the rest (over 1,4 million) was never attempted, so I am not certain as to why these were identified by the search engine. One should bear in mind that search engines work mechanically – they are not capable of discriminating. For this reason, one should not assume that the Web has 1,4 million URLs pertaining to the topic of smart cards. For the same reason, it is not unreasonable to assume that by using other key words, such as "IC cards" or "microprocessor cards", this could also have yielded a high number of "hits".

⁶ Entering the keyword "cartes à puce" (French for smart cards) yielded "only" 31 700 hits on the Google search engine, i.e. only 2,3% of its English equivalent "smart cards".

Making observations of the smart card community

The intelligent key to your quality of life – this was the message flashed with large, bright and piercing letters on a gigantic LED-screen that floated above the entrance to the "Cartes 2001" conference and exhibition in Paris, held in October 2001 – the first thing that caught your attention. This was indoors, in the mall of the mastodon CNIT-building; from the outside, the building looks like a hangar for jumbo-jets maintenance. The CNIT-building is located on the upper level of La Defense in Paris, right next to the steps that lead up to an imposing, modernist imitation of a triumphal arch. Still, the arch commands a panoramic view over Paris. It overlooks the La Defense, this modern business district where numerous multinational corporations have their European headquarters, in the high-rise buildings that surround the arch. Because of the security scare after the 11th September 2001 incident, all entrants steaming into this building had to show the contents of their luggage and handbags to a squad of security guards before they were allowed inside, into the mall. All the people waiting for this inspection were standing in a disorderly line waiting for their turn. Already at this point, the feeling of an itchy, vexing dampness and fatigue was taking hold – that uncomfortable feeling that starts creeping from the inside when you enter a warm room wearing warm, wet outdoor garments. Across the mall, underneath the gigantic screen (which now shows a new slogan: *Smart people use smart cards*), there is a new entrance to the conference and exhibition area located on three windowless floors below the mall. Reaching the first floors down, a dimly lit lobby emerges, guarding yet another entrance, this time to a large exhibition area. People are milling around the lobby – mostly men wearing business suits and carrying large briefcases; just as at the airport earlier in the morning, where they either were racing off to catch the morning shuttle to somewhere or racing off a still earlier morning shuttle from somewhere, now, this is their destination: They were crowding towards the desks in the lobby to register. As almost always, the persons on the other side of these counters are young ladies – they get total attention for the time it takes to complete the transactions involved at this point: Handing over forms, these being registered in the computers, the ladies scribble something on the forms and press some more keys on the computer, and then, with forced smiles, hand over a number of ID-cards, envelopes, receipts, brochures, books, etc. Or, they may pronounce: "Sorry, but you are not registered – exactly, how do you spell your name? I think you should register at the reception below". Following a hassle with various young ladies behind a number of different counters (Silent reflection: The robustness and persistence of French bureaucratic tradition and culture is formidable; it will outlive any smart card revolution!) around the receptions at different floor, a senior lady emerges from somewhere in the dimness: With an aura of professionalism she is able to find "monsieur's case" in the computer system by means of a few magic taps on the keyboard of her computer. All the while, for this one hour, the pressure from the itching dampness inside has been mounting, now I am openly perspiring, so much that the sweat is running down my forehead and fogging my glasses so I cannot read clearly the signs and directions that the kind senior lady, my heroine, instructed me to follow. So, I spot a dim, but quiet corner in the

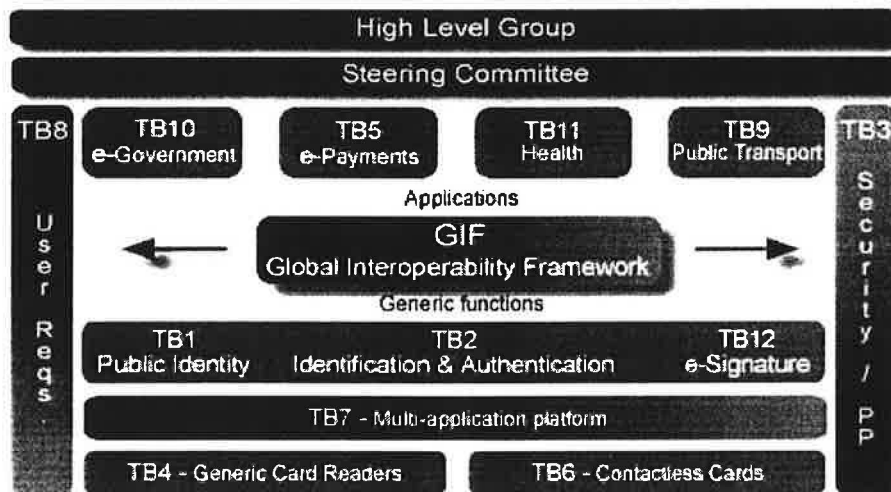
reception area where I strip off my clothes, down to my shirt, dry off sweat with a Kleenex. As typical of places like this, the air feels deoxygenized, instead it is filled with obnoxious plastic fumes mixed with odor of stale French fries. Yet people (all the men in their business suits and the young ladies) are cool, smiling, shaking hands, exchanging business cards and polite phrases of how are you and you look good and its been a pleasure; they seem to enjoy themselves at this annual, big-time event of the smart card industry. After a few minutes of meditation and cooling down, I ask myself: "What does this have to do with virtual keys?"

After three days of attending this conference and exhibition, my notebook was filled with observations and notes. The source of all this was from listening to presentations at seminars, talking to people attending these, participation on a "JavaCard Developers Day" – in addition to lengthy walks in the exhibition area, asking questions and eliciting explanations from representatives of the companies that had their own exhibition booths here. According to the organizers of Cartes 2001, there were 350 exhibitors present in the exhibition area, and they expected "13500 international professional visitors and 1500 delegates" to show up for this. In the catalogue of Cartes 2001, the companies with exhibition booths were classified according to "business categories" and "applications". Of the former, there were twenty main categories; some of these, such as the category "Technologies and solutions for local information systems, LAN and secure applications on the net" had five subcategories, e.g. "Secure applied software". This explains the strange feeling from walking around the exhibition area, in many ways similar to a Mid-East bazaar, but the content in the booths were a bewildering array of high-tech. Thus, afterwards, I had indeed collected a lot of data on smart cards and issues that the industry and its community are concerned with; my initial fears about the absurdities of going to Paris were unfounded. Paradoxically, in spite of this relief, I was also confused, so much information: Just as with entering the key word "smart card" in the Google search engine, attending Cartes 2001 had indeed resulted in an avalanche-like inflow of information and impressions. However, compared with a Web-search, the difference was significant: At Cartes 2001, real, breathing people mediated information. Most of the people I encountered were sympathetic, articulate and easy to approach, answering questions reasonably coherently, etc.

In spite of these differences in gathering information from the Web and being present, *in situ*, the problem of how to analyze and interpret these data (and all the other data collected in the project) remained unresolved: Obviously, these people, and the companies and organizations they work for, are actors or players in the construction, design and diffusion of the virtual keys. Their main interest is the expansion of the smart cards markets, but, to summarize a sentiment (not overtly stated): They think this diffusion is going too slowly, especially in the USA; they want the demand for smart cards to take off, to increase exponentially – and they are searching for ways this may happen. Some advocate more standardization and international cooperation ("Japan!"), others think that promotion of multiapplication smart cards is the best strategy, however, this will demand a high degree of cooperation from different players. Some hint that the "War against terrorism" is a golden opportunity, it will generate a large demand for "secure" keys, i.e. PKI, biometrics, ID-authentication, etc. Others, especially the large players, enthusiastically claim that their

solution and technology will promote all this, their message is “buy our products because we are the best”. The more pessimistic (there are some) lament the fact that a “killer application” is still lacking for smart cards – they repeat the cliché that “smart cards is a technology looking for a solution” and that the industry has to face the fact that none have been able to develop a convincing business case for smart cards⁷: Smart cards are still too expensive and inconvenient in use, they claim. The pessimists advocate more hard work, however, in spite of being vague as to what this implies, listeners in the audience nod approvingly and give generous applause as endorsement to this type of message, just as they did with the enthusiasts.

The next scene is six weeks later, this time within a building of the ETSI – the European Telecommunications Standardization Institute – located on the beautiful hills above Antibes, not far away for Nice on the French Riviera. (Recall some of the landscape paintings of Paul Cezanne – the view from ETSI looks similar.) This time, it is the biannual meeting of the “Smart Card Charter” of the “eEurope”-program, which is promoted by the European Union. Of course, there is a hidden agenda in all this: The Europeans, specifically the French, want to become world leaders of the smart card industry. At the meeting held at ETSI, participants of the various “Trail-Blazers” organized by the Smart Card Charter have project meetings and discuss their plans⁸. There are twelve “Trail-Blazers”, or TBs, the euphemistic term used for projects, covering different aspects of smart card development, such as TB1 on “Public Identity” or TB12 on “Advanced Electronic Signature”. The exhibit below, copied for the home page of the SmartCard Alliance, shows how the organizers envisage the structure and relationships of the twelve TBs. (Notice its structural similarity to the ISO/OSI reference model.)



⁷ That is, except for its formidable success as SIM-cards in mobile telephones, but they seem to disregard this, maybe because this is not their “baby” and the growth potential has saturated.

⁸ For more information, consult: <http://eeurope-smartcards.org/trailblazers.htm>

At the ETSI-meeting, there was no exhibition, just project meetings and related politics/negotiations, the latter often guised behind a veil of “technical requirements”. This time, attending the TB7 on multiapplication smart card, more so than at Cartes 2001, the engineering design approach dominated the presentations and debates – all this mediated by power-point presentations that numerous participants apparently had in their lap-tops. Thus, the attention of the participants was divided between the power-point presentations on the big screen and what they were writing into their own lap-tops. Each new presentation went through the motions of connecting the projector and power cables to the lap-top, switching on the computer, waiting for this to “boot-up”, searching in the file directory, etc. Then, the power-point presentation started: Boxes, circles and arrows flashed on the screen, some with animation (favorite: arrows that fly into the picture and land as connections between boxes), claims and statements neatly written with bullets on their left side. Some of the presenters used hand-held LED-flashlights emitting bright, red spots as pointers. Revised project plans were presented, people around the table nod affirmatively, until one of the more senior participants, looking more and more distressed, finally breaks into the discussion, asking: “What is the real advantage with smart cards for those who are potential smart card issuers?” He appeared irate, almost barking, he continues: “Are there any card issuers who are interested in multiapplication cards?” All of a sudden, the discussion is dislodged, it becomes disorganized, as some tried to answer by repeating what they had just presented, while others supported the critic by expressing concerns about “lack of a clear business case” and asking “who is really interested in smart cards?” – “anyway, the costs of smart cards are still too high!”, etc. Just as fast as the breakdown of the façade of certainty regarding the future prospects of smart cards had hit the meeting, so this was restored, as the chairman called the meeting to recess, because “now is time for lunch, we need lunch now, because we have a demanding agenda for this afternoon”. When the meeting recommenced two hours later (French lunch), the pre-lunch crisis was not mentioned; the presenters continued with their power-point presentations, and the meeting was adjourned late in the afternoon (6 p.m.), with the following cryptic statement by the chairman: “I think there is a need for consolidation of the eEurope initiative”.

According to Jan van Arkel, who is the co-chairman of the steering committee of the Smart Card Charter, about 1000 individuals are connected to the eEurope Smart Card Charter’s activities, involving more than 300 organizations in which 250 persons are working “hands-on” with smart card development projects associated with the various “Trail-Blazers”. The result of this is evident mainly in documents and power-point presentations (what is often called “deliverables”) that recommend actions believed to promote the development and diffusion of smart card technology. In spite of all these activities, there is something confusing and unresolved, as evident in all the proposals for how a “real” business case should be made for smart cards, or all the conditions and prerequisites that have to be arranged in order to create a “killer application” based on smart cards. Thus, after three days of mostly listening, but also talking to, these developers of smart card solutions, the feeling emerged that these people are ambivalent as to their prospects of succeeding with their projects. Simultaneously, they are avoiding the topic of why SIM-cards have been successful

– and the role of the mobile telecommunication industry. This is strange, as the meeting was held at ETSI, hosted by ETSI. ETSI, as an organization of the telecommunication industry and authorities, has a long experience in smart card development, in particular system design and specifications. Thus, in leaving ETSI and the beautiful Cezanne landscapes at the end of the meetings, I am loaded with a notebook full of empirical data in addition to a number of kilos of documents and other publications, but I am still confused: There must be a profound political and economic dynamic, or, maybe a contradiction, underlying this situation: Apparently, no one wants to take the risks of being a first mover, as there are “no obvious business cases”. Simultaneously, everyone thinks that smart cards may provide numerous benefits – they are essential for eEurope, for numerous industries, for national and private security, for the promotion of democracy, and a host of other important issues. In brief, the future information society is in dire need for virtual keys. Smart cards have the potential of providing just this, and a host of other beneficial solution, the enthusiasts claim. Yet, they are hesitant and ambivalent as to how this goal should be attained – they seem to lack confidence. This then became the starting point to find out why: In this report, I shall try to explain the complexities involved in this – why design, construction and diffusion of smart cards as virtual keys are intertwined and reflect the complexities in how society and ICT technologies interact.

Plan of this report

Having explained the purpose and ambition of this report and how the inquiry was undertaken, the scene is now set: In the next chapter (chapter 2), a number of different theories and approaches relevant for the explanation of technological construction will be presented and discussed. The aim of this is to identify to what extent these are fertile, or to what extent or why these are unsuccessful in explaining the development and diffusion of ICT. Following this, the next chapter (chapter 3) will focus on virtual keys and smart card technology. Because the latter is important for some implementations of virtual keys, the chapter will describe and explain in terms of technical aspects and applications, i.e. how the smart card technology is used. The main theme of the following chapter 4 is the question of whether virtual keys represent technological discontinuity or continuity. This is an important question in terms of contested claims that the impact of ICT is significant because it represents a cluster of radical innovations. Pointing to antecedents and predecessors, sceptics disagree, claiming that technological development is ruled by continuity. The diffusion of virtual keys qua smart card technology has been uneven, i.e. rapid in some areas – slow in others. Exploring this is the topic of chapter 5, which also presents the results of a group of people who are influential in the diffusion of smart card technology, i.e. the results of an in-depth survey of seventeen project leaders of large smart cards projects in Norway. An important aspect related to the application of virtual keys is money, specifically, the pervasiveness of electronic money in modern society. This topic, which is important for understanding the construction and diffusion of smart cards, will be presented in chapter 6.

Finally, in the conclusion, in chapter 7, the results of the inquiry will be analysed and discussed in view of the initial claims made in chapter 1 and chapter 2. Bon voyage!

2 Theories explaining construction technology and ICT

Introduction: Explaining ICT construction as virtual keys

Contemporary explanations of how technology is created are influenced and informed by theoretical approaches that were developed prior to the emergence and strong diffusion of ICT, which began in the 1980s and became pervasive in the 1990s. Initially, I claimed that there is a need for new ways of explaining how technology, in particular ICT, is created. Although many, if not most, established theoretical explanations provide interesting and illuminating explanations of some aspects related to how ICT is created and developed, in terms of explaining salient characteristics of ICT, they are usually fragmentary, in fact only partly successful. The ambition of this report is to discuss and suggest other, alternative explanations and strategies for inquiry. The main vehicle for this will be the presentation and analysis of the virtual keys in the following chapters, in which the main focus will be on the development and diffusion of smart card technology. However, as this case study is motivated by the quest for new ways of explaining how technology, in particular ICT, is created, designed and developed, this claim needs to be justified and elaborated. This will be undertaken in the following sections of this chapter. First, I will briefly explain why statistical and taxonomic approaches to ICT, although interesting and illuminating, mainly provide insights in terms of broad, aggregate characteristics related how ICT is created. Following this, I shall continue by reviewing some of the mainstream explanatory strategies used in theoretical approaches to design, construction and diffusion of technology – and attempt to identify their strengths and weaknesses.

Technological construction in the ICT sector: The landscape, facts and taxonomical approach

The magnitude of work undertaken and resources allocated to creation and construction of novel technologies in the ICT-sector is considerable. Figures showing the precise size of this on a global scale are not available, however, some statistics give a clear indication of this, such as the figures from the Washington-based Industrial Research Institute (IRI). IRI reported⁹ that in 1999, the US industry spent US\$ 87,3 billion on R&D related to ICT, this possibly being the largest R&D area in the world. In addition to this, there is a substantial R&D effort in ICT undertaken by various public organizations in most OECD member countries, such as universities and research institutes financed with public money. On average, the size of R&D in proportion to the US companies' revenues in the IRI-figure was

⁹ Cf. "20 Largest R&D Spending Industries in 1999 and 2000 (by SIC Group)", *Research-Technology Management*, Sept-Oct 1999, p. 8.

10,3%, which is high, making these companies R&D-intensive. The figure quoted above encompasses a broad range of R&D-activities, which in the IRI-figures are classified according to the type of products in which the R&D is undertaken. In this, R&D on telecommunications equipment and software constitute the largest areas of R&D. Although US companies have a leading role in the development of ICT, there are numerous large companies outside USA in the ICT-sector and these are also R&D-intensive. In 2001, Nokia, with HQ in Finland, had an R&D budget of US\$ 2,3 billions (approximately 10% of its revenues) – the R&D was undertaken at numerous labs around the world, of which two were in China. Possibly, more than 1 million persons work with R&D related to ICT around the world. Thus, a fair assumption to make is that the population of people who work with innovations (typically R&D) in the ICT-sector is considerable – the majority of this effort is undertaken in the industry; ICT-firms invest heavily in R&D because they believe that creation of their own, unique innovations will make them competitive and provide them with future profits and competitive advantages.

Behind the figures above, the scope and variety of R&D undertaken in the ICT-sector, hence the type of technological construction carried out is not known precisely; however, it seems fair to claim that this constitutes a heterogeneous group in a number of dimensions. In her analysis of technological construction and design, Vivien Walsh (Walsh 1995) classifies the work undertaken according to the disciplines, crafts and skills of the people involved in a product development process. This type of approach is attractive because it may explain why firms are able (or unable) to create unique innovations; however, there are few, if any, statistics that provide figures according to this type of classificatory scheme. Still, as evident in numerous annual reports, press releases and presentations made by R&D-intensive firms in the ICT-industry, there is a tendency towards greater variety of the disciplines and skills mobilized by firms for the purpose of undertaking technological construction and design; increasingly, firms establish cross-disciplinary, inter-departmental, special purpose product development teams, typically organized as projects or programs, i.e. as organizational entities that exist for a single, finite purpose. Furthermore, even if many R&D-workers classify themselves as engineers (because they have a basic education in engineering), in the course of their work they become so specialized that traditional academic criteria of categorizing their skills and mode of work are not accurate. In addition, R&D-organizations increasingly recruit people with non-engineering backgrounds, such as people educated in liberal arts, because firms realize that their skills and insights are important for product development, i.e. product development, they realize, has to be market oriented, essentially this is construction of social and cultural technologies, not just machines. Thus, the challenge of technological design and construction is to understand and interpret confusing, inarticulate market signals, signals from users and customers who may be faithless, capricious, irrational, impulsive, etc. For this reason, a multitude of disciplines and skills are mobilized in the course of technological construction – increasingly people with knowledge and focus on humans, cultural and social systems, behavioral patterns, etc. are incorporated in efforts of technological construction.

Instead of focusing on statistics for providing greater insight to the landscape of technological construction in ICT – which in any case is futile because of the incompleteness

of statistics – a potentially more promising approach is to give attention to the types of innovations that these efforts are aimed at. In this, in spite of its heterogeneity, innovation theory may provide guidance. Thus, the typological distinction that some innovation theorists (e.g. Chesbrough and Teece 1996; Utterbach and Suarez 1993; Abernathy 1985) make between *system innovations* and *autonomous innovations* may be useful for understanding important characteristics that differentiates technological construction and design in ICT. The former category, system innovations, may adequately identify and characterize people who work with development, construction and design of novel ICT-systems, or upgrading of existing systems, i.e. the large “ICT-machines” such as the development of the GSM mobile communication system or computer communication systems used by banks and airlines. Their perspective and focus will to a large extent be on the system, i.e. how it works, its functions and users, the equipment connected to the system and its software, its capacity, mode of work and specific characteristics. An alternative term for this could be “infrastructure related technological construction” because these large systems constitute infrastructures. Thus, technological construction, such as development of routers, communication software or cables, is related to the systems they will be integrated into, which transcends the typologies used by the equipment manufacturing industry and which constitute the categories used in statistics, such as IRI’s figures on industrial R&D. In contrast to system innovations, autonomous innovations are, as the term implies, independent of others, such as an outboard motor, a bicycle, a can opener or a PC that is not connected to a network. ICT and the technological, physical elements that constitute ICT, is system dependent. In analyzing this, the concepts of *complementary technologies* and *complementary innovations* may be fertile, because these recognize the interdependence of the elements that constitute an ICT system, as evident in peripheral equipment connected to a communication network, such as a PC used as an Internet terminal or a mobile telephone handset. The complementarity aspect of these is based on the mutual interdependence between the system and the technologies that are connected to the system – this interdependence being so essential that removal of one element makes the system meaningless, the system cannot exist without the complementary technologies.

With the technological convergence that underlies the growth of ICT, the degree of complementarity of various elements related to a network or system has increased; in fact, the concept of convergence is another way of depicting increased complementarity. Simultaneously, making a distinction between system technologies and complementary technologies has become difficult, perhaps also less meaningful. This may be illustrated by an example: In the GSM mobile communication system, the software employed resides physically in many elements, such as in the base station, in the switches and exchanges, and in the mobile handset. In establishing a communication session (e.g.: A talking to/interacting with B), a long chain exchanging information back and forth is activated by the software residing in the various elements. Physically, one may claim that the mobile handset is autonomous (that’s why it is called mobile), however, logically and functionally, the handset is firmly integrated in the system, for which reason the handset may be viewed as complementary, not autonomous.

For the usual user of an ICT-system, the point of interaction goes through a terminal, i.e. by means of the complementary technology, or to use technical terminology, the human-machine interface. For this reason, constructing these types of complementary technologies poses different challenges from those related to system construction, even if these are closely interdependent. The virtual keys may be analyzed as having a position in-between complementary and system technology. Technically, these work as switches that turn on and off access to the system for the user, for which reason they may be classified as complementary technologies. Some of the keys, even if they operate in a virtual world, have a material embodiment, e.g. as a magnetic stripe or an integrated circuit in a smart card. Other keys are completely immaterial because they are based on passwords that users memorize and try to keep secret. Still others, the biometric keys, are based on the idea that information on the users' bodies, such as fingerprints, is individually unique – making the body a medium for information that function as a key. Most of the virtual keys are usually combinations of a password or PIN-code and some kind of physical medium. Analytically, using mechanical keys and locks as precedents, one may claim that the system constitutes the lock as this is “opened” by the virtual keys, i.e. what may be termed a complementary technology. However, this is simplistic, because keys and locks are interdependent. Furthermore, as evident in smart cards, these keys may even be considered as systems because of the software, memory and processing capability that reside in the integrated circuit in the smart card. Thus, when a smart card is inserted into a card reader, the function of a key is but one of numerous applications of the card. In a sense, the roles are reversed, because the card reader and the system this is connected to may be considered complementary to the smart card. This may be illustrated by the “health cards”, the type of smart card that store personal, private medical information of the patient in the card's memory. In this case, when the card is inserted in the physician's card reader, the ICT-system of the clinic becomes a terminal that serves the system residing in the smart card.

The implication of this is that categorization of technological constructions and innovations using substantial characteristics is not obvious and does not provide significant explanations; categories become fluid, depending on a particular situation, as evident in the discussion above on the distinction between system-related, autonomous and complementary technologies. This may be explained as an effect of ICT's composite nature, i.e. the combination of equipment and physical infrastructures that function in a totality, as medium for non-material phenomena – symbols, information, narratives that are mediated electronically or, increasingly, by means of light in optical communication networks. However, for the people who work with creating and designing these technologies, such analytical difficulties are probably irrelevant; if asked, they would probably think: “How foolish!” Their conception of what they do is probably concrete, tangible, even if this has a non-material manifestation, such as doing software development. For this reason, they will have a clear idea of their goals, the objective of what they are doing: They are creating new technology – something novel that has to work and function, preferably something that users will love and desire. Thus, it may be fertile to ask: If the statistical and typological approaches

do not provide satisfactory explanations of how ICT is created, are there other approaches that may provide better insights? Below, this will be explored.

Mainstream explanations of technological construction

In contemporary explanations of technological construction, two approaches or explanatory strategies have a major position. These two may be labeled as: Optimization theories and social constructionist theories. However, in addition there are numerous, more specialized explanatory approaches that to some extent are influential. Explaining the development and diffusion of the new, electronic keys and locks, especially the smart cards, in terms of these theories is not straight-forward: Some aspects are satisfactorily explained by one approach, however, other aspects are explained more successfully by rival, almost antithetical approaches. The exhibit (figure 1.1) is an attempt to represent this theoretical landscape, i.e. the various approaches that exist in terms of understanding and explaining how technology is constructed.

One of the major approaches, the “optimization theories”, advocate pragmatic and rationalist explanations, i.e. straight-forward explanations that focus primarily on technological construction as an instrumental, technical-economic question. Among practitioners of technological construction, especially among those with an engineering background, the rhetoric and reasoning in optimization theories are often mobilized in their justifications. Herbert Simon (Simon 1969; Simon 1992) has called this approach “the science of the artificial”, because in technological construction, the main challenge is to develop solutions that are the “best possible”, or *optimal*, in terms of expected output in relation to costs and input resources needed for creating a new product or service. The basic tenets of this explanatory strategy have become a foundation for a considerable management oriented scholarship and literature aimed at prescribing ways and means for improving technological construction. In this, questions related to *what* is created by technological construction and *why* some solutions tend to be more favored than others is not given much attention apart from aspects related to input/output, i.e. considerations of efficacy or profit, and how this may be achieved.

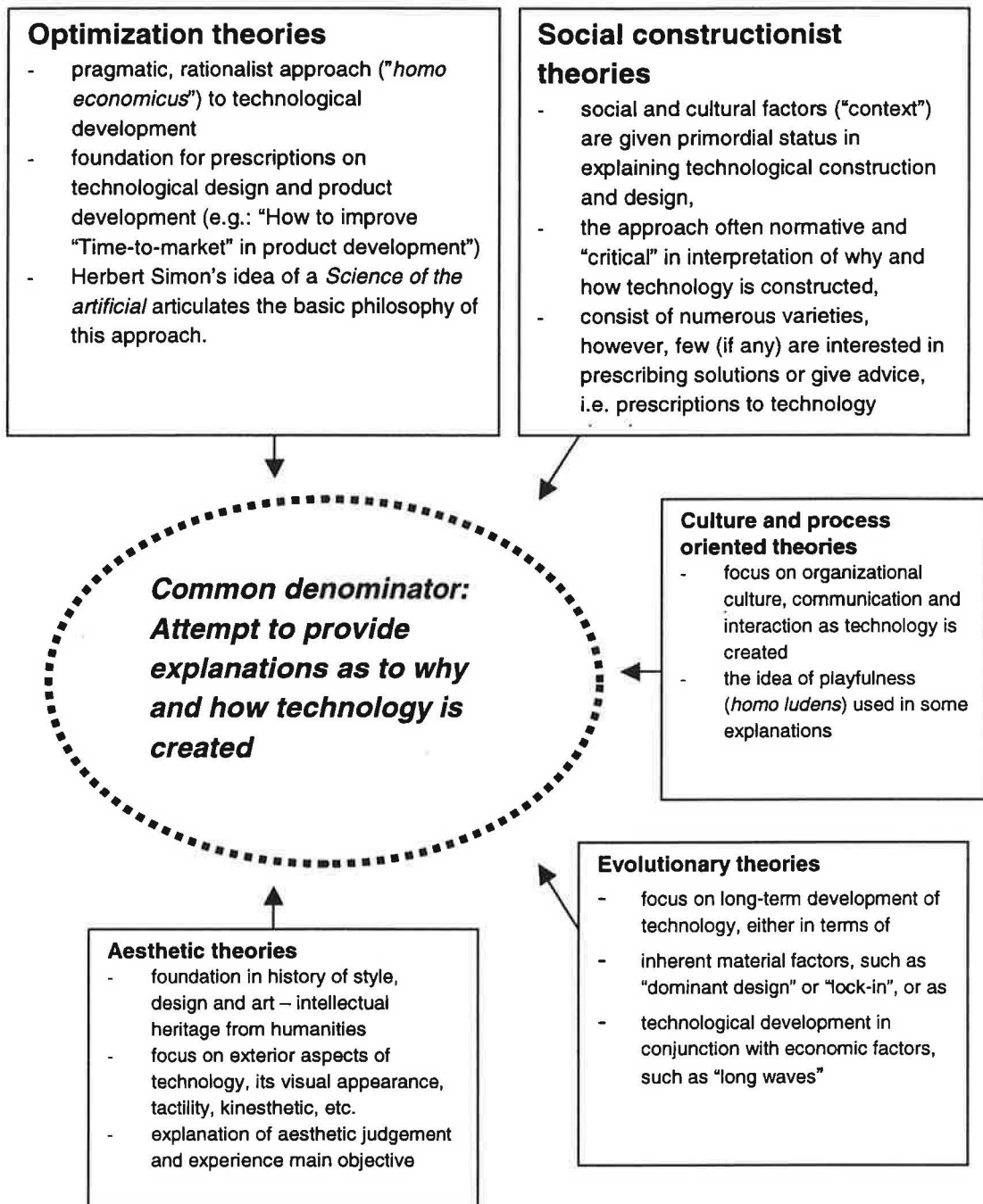


Figure 2.1: Overview showing the most common theoretical approaches in explaining technological design and construction

The other major approach may be found under the broad label of "social constructionism". The approach is heterogeneous because it consists of numerous varieties, however, they have a common focus and position: First of all, they claim that explanation of why technology is constructed and diffused has to be sought in social and cultural factors – these factors have a primordial status; the explanations promoted by others, such as the optimizationists, may at best be considered secondary, more specialized explanations. Accordingly, understanding the

context in which technology is created or taken into use is the primary concern in explanations. The methodological implementation of this in research and analysis is, however, a matter of great variety and internal dispute. The social constructionists entered the arena as a refreshingly novel, dynamic force in the early 1980s because its pioneers had great success with employing anthropological methods in the famous "laboratory studies" published at the time, cf. Knorr-Cetina (Knorr-Cetina 1981), Latour & Woolgar (Latour and Woolgar 1979).

In addition to the major approaches, there are three other approaches of interest and relevance: Whereas two of these are related to the major approaches identified above, a third approach has a more autonomous position. Labeled "aesthetic theories" in figure 1.1, the latter has a long tradition in academic disciplines such as history of art and architecture, philosophy and aesthetics. This approach is significant for analysts who consider technological design and construction as an aesthetic activity, something that explains style, designers' decisions and intentions, and their *modus operandi*. (Ferguson 1993; Malmanger 2000; Seippel 2001). The insights provided by this approach are distinct from the others as they employ a style of argumentation, with expressions and terminology that may be unfamiliar to most students of technology. Still, these are interesting because with their focus on aesthetics, they are able to explain important factors that are often overlooked and ignored by the other approaches. The aesthetic factor, although unrecognized and often hidden or camouflaged in the rhetoric of technical-economic discourses, is nevertheless very much present when new technology is created. Furthermore, it is important in the diffusion of technology, most obviously as fashion. In addition, it is also concerned with why there are distinct styles of technology.

The other two, minor approaches are affiliated with the majors, however, they are sufficiently distinct so as to justify autonomous categorization. One of these, the evolutionary approach, is also diverse and heterogeneous in terms of explanations and analytical foci, however, the strength of this approach is that they offer the "big explanations" of how technology and society interact and co-evolve, as evident in the attempts to explain long waves (regularities) in techno-economic development, (cf. Freeman and Perez 1988; Dosi 1988; Mokyr 1990; Rosenberg 1994). A more technologically "pure" variety of this approach attempts to explain technological evolution in terms of inherent material and structural characteristics of innovations and their development, (cf. Utterbach and Suarez 1993; Sahal 1985; Abernathy and Clark 1985; Vincenti 1995). As evident in their name, evolutionary explanations are inspired and informed by biological evolutionary theories; analogies of the key concepts such as "mutation" and "selection" are often used in order to explain how technology is created and established. Because of their technical and physical focus, the advantage of these approaches is their ability to explain what are the technological limits and rationales in various developmental trajectories.

The second minor approach, labeled "culture and process oriented" theories, is interesting because in this, the main focus is set on explaining how work related to technological construction and design is undertaken, cf. (Bucciarelli 1988; Dubinkas 1988; Feldman and March 1981; Henderson 1991). Although one may claim that this approach is really social constructionist, which in many ways it resembles, it differs from this because its

research agenda has a clear empirical focus on aspects related to work organization and culture, aimed at providing explanations of how work processes and related factors determine the outcome, i.e. the construction of technology. Because of this, this approach is also interested in the playful and aesthetic aspects of doing technology construction – an interest they to some extent share with those working within an aesthetic theoretical framework, the third minor approach identified above.

As evident from the brief overview presented above, a multitude of theoretical approaches exist in terms of explaining technological creation, design and construction. These differ from each other mainly because they emphasize and focus on different aspects related to how new technology emerges. This in turn may reflect different academic disciplinary cultures (e.g. economist focus on economic aspects, etc.) and identities, but also different epistemological positions. In addition, differences may be amplified by idiosyncrasies related to their discourse culture, as evident in the type of terminology and key concepts they choose to use in their analyses.¹⁰ The two major approaches – optimization theories and social constructionist theories – deserve closer attention because they are influential, far outside the academic communities that host these. Below, in the next two sections, a brief analysis and review of these will be undertaken.

Optimization theories

In writing about the science of the artificial, Herbert Simon claims that: “Everyone designs who devices courses of action aimed at changing existing situations into preferred ones” (Simon 1969, p. 55). The preferred situation implies creating an *optimal solution* to whatever is perceived as a challenge or problem. This ideal holds a strong position for justifying how and why technology is created among theorist who may be broadly classified as optimizationists. The core idea in creating an optimal solution is to achieve a balance between an internal construction or design (e.g.: a machine, device, procedure, etc.) and the external environment. When and if this balance is achieved, the solution may be characterized as optimal. With his theory of a *science of the artificial*, Herbert Simon (Simon 1969) articulates the basic, general tenets of design. He is still influential; his name and, even more, his arguments are still called upon by many contemporary analysts as an authority on the fundamentals involved in technological construction and design. In elaborating his theory, Simon makes an interesting distinction between science (especially natural science) and those disciplines and professions that provide solutions or create something, such as engineers, dentists, lawyers, teachers – and, not the least, craftsmen and others who possess problem solution skills (e.g. plumbers, mechanics, cooks, etc.). Whereas the former, scientists, strive

¹⁰ Cf. Karin Knorr-Cetina Knorr-Cetina, K. D. (1981). The Manufacture of Knowledge - An Essay on the constructivist and contextual nature of science. Oxford, Pergamon Press.

Lagt inn 2/3-2000 i forb. med designessay uses the expression “fabrication of a scientific fact” to depict how scientific results are made. Understandably, some people may think this as insulting and misleading.

for understanding and explaining nature, the latter are basically dealing with creating something artificial, i.e. something made by human beings¹¹. For Herbert Simon, the notion of artificial is a neutral term¹²; the purpose of design is to create something artificial. Following this, he defines design as “..how things ought to be, with devising artifacts to attain goals” (Simon 1969, p. 59). The challenge of design is to create a balance between an inner environment (the designed artifact) and an external environment: “The optimization problem is to find an admissible set of values of the command variables [i.e. alternative solutions], compatible with the constraints, that maximize the utility function for the given variables of the environmental variables” (Simon 1969, p. 60). Following this, Simon specifies that the science of the artificial must use:

- utility function theories and related statistical tools in order to create a logical framework from which to choose alternative solutions,
- develop methods and techniques for making visible which solution is optimal,
- adapt a “standard logic” to be used for finding what solution is optimal,
- develop quantitative methods aimed at rating differences between possible, alternative solutions,
- allocate resources in order to develop or simulate solutions that are not well understood.

The core in Herbert Simon’s thinking about design is utilitarian, i.e. maximization of utility as the guiding principle of all design. For this reason he thought that designers should have a common methodology. These assumptions are identical to those found in economic rationality, in the idea of *homo economicus*. The advantage of this approach is its neutrality as to what constitutes utility; the assumptions do not (in theory) impose moral or aesthetic norms or discriminate, as utility is something defined by each actor – a judgment made by each actor.

More than thirty years have passed since Simon wrote his seminal essay on the science of the artificial. In some ways, the ambitions that Simon spelled out have become within realistic reach due to the rapid development of computer-based simulation and visualization methods. In terms of design and product development, computers are now utilized in rapid prototyping machines and in various sophisticated representations of complex processes. Thus, designers are able to base their decisions based on data that give a high degree of certainty as to alternatives, as Simon admonished. Still, as these tools have developed, the complexity and difficulty of these ambitions have perhaps become clearer. An interesting, paradoxical development may also be observed in the rival social constructionist theoretical

¹¹ A somewhat similar distinction, however, using a different taxonomy, may be found in the theories that claim that modern knowledge production systems consist of two disparate modes, “Mode 1” and “Mode 2”. In this, Mode 1 is equated with the academic type of knowledge system, whereas Mode 2 is found outside academic, mainly in the industry and consultancies (cf. Gibbons 1994; Gibbons et al 1994).

¹² Possibly, Simon may be interpreted as having a positive idea of “artificial”; in the text, it does not have a negative connotation. In colloquial English and many other European languages (e.g. “künstlich” in German), the expression “artificial” also carries a derogatory connotation as it may imply insincerity, hypocrisy, falsehood, such as in the statement “He seemed artificially friendly”.

trend that emerged in the early 1980s: In his justification of the concept of “artificial”, Simon claims that the distinction between artificial and nature is fluid and ephemeral, because “..those things we call artifacts are not apart from nature” (Simon 1969, p. 3) – artifacts serve as the link between nature and human beings. This claim is similar to some of the assumption that underpin social constructionists’ reasoning, as evident in the work of Bruno Latour (Latour 1992) in his notion of an actor-network theory. According to this, the distinction between culture/society and nature is fluid; thus technology is created as negotiations between society and nature.

Even if one may observe similarities in some of the basic assumptions in both optimization theories and social constructionist theories, they are very distinct in terms of discourse culture and institutional affiliation. Furthermore, within the rich and abundant literature and scholarship informed by the optimization theories, it is possible to distinguish two distinct grouping using similar criteria, in terms of their approach to product development and technological design: The *technological approach* and the *management approach*. In spite of differences, which will be briefly explained below, the two approaches share some of the basic tenets and strategies for justification. The differences between these two varieties of optimization theory are most apparent in terms of rhetoric, i.e. their discourse culture. More specifically, the technology approach puts a greater emphasis on understanding and explaining technical and operational aspects related to the design and construction process. In this, they tend to mobilize a rhetoric from natural sciences and engineering. In the management approach, greater emphasis is put on economic aspects, i.e. making prescriptions as to how to increase profitability in the design and construction process. In this, market analysis has an important role. Thus, they tend to use a business world language in their discourses. Whereas the technology approach has its base in the engineering design and natural science departments of the academic world, the management approach typically belongs to business schools and related consultancies, however, this distinction is blurred as one may observe a considerable overlap in the affiliation and rhetoric of the two approaches.

The two approaches are united because they have a common agenda: What characterizes or causes a successful technological design and construction? Furthermore, they are similar in their strong emphasis on providing prescriptions or advice to its audience as to how success should be achieved, or, conversely, how to avoid failures. Being normative in this, they have in common a strategy of rhetoric: A prescriptive instruction (i.e. what should be done, and how) is put forward, followed deductively by arguments as to why. The type of arguments that are offered are often common-sense, supported by slightly ideologically or politically tinted paroles, as evident throughout Lars Hein and Mogens Myrup Andreassen’s influential book on Integrated Product Development (Andreassen and Hein 1986)¹³, or in the Stage-Gate-model created by the product development guru Robert G. Cooper (Cooper 1996;

¹³ Cf. pp. 92, 93, 141, 166, 169 for a few samples – one of these admonish “A (product development) project which fails must be terminated prior to production and sale!” (p. 166) [translated from the original text in Danish].

Cooper, Scott J. Edgett et al. 2000). In reading their texts, another striking difference from other theoretical approaches is their use of graphics in their discourses – diagrams, flow-charts, etc. inserted with headlines of prescriptions and parables. A point of difference in the two approaches may be found in their emphasis and prescriptions on how to organize, in particular how product development should be undertaken. In the management approach, as evident in Cooper's Stage-Gate-model, great emphasis is put on market research and testing throughout the product development process. In addition, it recommends giving projects a high degree of autonomy ("empowerment"), however, this being subject to strict supervision by the firm's top management, specifically by the product manager. In the technological approach, more emphasis is put on evaluation of technical aspects in the product development process. However, this approach also recommends establishing cross-disciplinary, multi-skilled project teams with a degree of autonomy, but the exact power-structure of the projects is not specified to the extent found in the management approach.

In general, the optimization theories do not ask why a particular technological solution was chosen, what really constitutes optimality; this question is relegated to the markets: If something succeeds (e.g. sells well in the markets), the decisions made in designing and construction must be right, hence optimal. In the various approaches that belong to the optimization theories, it is difficult to find satisfactory explanations or inquiries as to why and how technology is created, beyond the assumption that construction and design of new technology is undertaken to make improvements and novelties that society will take into use, i.e. a question of the utility function. Questions such as: What inspires a designer or makes him or her develop an idea? What makes the designer choose and develop a particular design, instead of other possible, when other, rival designers choose differently – all claiming their choice to be optimal and rational? If a novel product or construction becomes successful in the markets – is there an agreement between the users/consumers and designers as to what constitutes optimality? What is the difference between a consumer's sense of satisfaction and a designer's idea of optimality? Or, more generally, what makes society adopt or require specific technological solutions, and how do designers interact with these in their work? These questions and a host of others questions are difficult to answer following optimization theories, however, following their advice may often prove to provide good support for those who struggle with creating design and constructing technology.

Social constructionist theories

In the early 1980s, a refreshing, novel approach – usually calling itself social constructionist - emerged in the landscape of theories explaining technological construction and design. Their initial success was due to their credible descriptions and penetrating analyses of science and technology in the making, in the famous "lab-studies", which were based on empirical data from close observation and contact with informants in laboratories. These analyses served as a platform for a critique of idealized and highly stylized notions about how research and development is undertaken, and in particular how scientific knowledge becomes created. The

pioneers of this, such as Karin Knorr-Cetina (Knorr-Cetina 1981) and Bruno Latour and Steven Woolgar (Latour and Woolgar 1979) gave the initial push for establishing this as a strong academic discipline, under the label of STS – science, technology and society studies – which have now become firmly established and institutionalized, mainly at universities.

Compared with the optimization theories, there are numerous characteristics that make social constructionist theories distinct. First of all, even if critical, they position themselves in academia, as interpreters and producers of knowledge about society. In comparison with optimizationists, they lack ambitions in terms of contributing towards “progress” in the design and construction of technology – the strong, well-intended prescriptions found in the optimization theories are absent among social constructionists. In fact, numerous analysts are critical or pessimistic of the “modern project”; for these, modern technological construction and design epitomizes the evils of modern, industrial civilizations and economic system, as evident in the works of Brian Wynne (Wynne 1975). Thus, some have a clear political agenda, however, others, such as Bruno Latour, claim that they are merely “agnostic”. Social constructionist seem attracted to analyzing cases in which research or development projects have failed, or became scandalized or caused great damage. Secondly, perhaps more fundamental in term of difference: Social constructionist claim that creation and design of technology may best be analyzed and understood in terms contextual social and cultural factors; technology is created due to social causes, not the opposite, which they characterize as misconceptions of “technological determinism” or “essentialism”. In their view, technology articulates and mediates power, politics, gender, beliefs, etc., i.e. factors that constitute social systems and cultures. Thus, the concept of “the social shaping of technology” (Bijker, Hughes et al. 1987) potently labels their idea of how one should explain design and diffusion of technology.

Although one may be sympathetic to this basic position of the social constructionist approach – after all, technology is undeniably result of human efforts – there is something unresolved in the results from this approach. This claim may be considered unfair because in the scholarship undertaken by this large and heterogeneous community, there are numerous outstanding analyses that provide rich insight, especially in-depth case-studies, into how technology is created and science is undertaken. Thus, in reading these, one feels almost present or in-situ, in the laboratory or close to the desk where the engineer designs his or her machine. Perhaps the strength of their approach is simultaneously their weakness; their contribution to explaining why technology evolves is theoretically meager, almost banal. This has been pointed out by numerous critics, perhaps most eloquently articulated by Langdon Winner, who writes “..that although social constructivists have opened the black box¹⁴ and shown a colorful array of social factors, processes and images therein, the box revealed is still a remarkably hollow one” (Winner 1993, p. 448). In Winner’s view, the most serious implication of this is that they do not contribute politically or normatively; their lack of prescriptions or “agnosticism” is at best academically introvert, possibly nonchalant, in spite

¹⁴ Winner uses this term (black box) to designate technology or science that is complex and difficult to understand for non-specialists – and which are de-mystified by the analyses of this type of research.

of their aura of “critique” and “reflexivity”. Alternately, one may claim that this weakness has emerged because they are struggling with developing a coherent theoretical superstructure. This is evident in a number of analyses that some prominent members of the social constructionist community have published, and which will be briefly commented in the following.

The latter claim is evident in the colorful and vivid writings of Bruno Latour. The core of his theory is the idea of actor-network theory (acronym: ANT), which he has attempted to strengthen by adopting an analytical approach from linguistics. The key concepts in this is his notion of “program” and its dichotomy “anti-program”; Latour claims that engineers “inscribe” technology with programs that attempt to control or manage the behavior of its users¹⁵, as a delegation of functions undertaken by humans to machines (Akrich and Latour 1992, p. 260-261). Conversely, people will attempt to circumvent these programs, hence their “anti-programs”. In his original way, Latour illustrates this with the case of a “Berlin key”, a special type of key that forced tenants of apartment buildings in Berlin to lock the gate door from the street outside, each time they left the building (Latour 1992). By employing the dichotomy of a syntactic dimension and a paradigmatic dimension in analyses, Latour claims that this approach is “convenient” because it is then possible, as in a linguistic analysis, to substitute one element in the two dimensions, whereby an entirely new picture emerges. This is akin to what Latour claims linguists do in their analyses, i.e. that a change in some elements are syntax-wise more profound than others. Transferred to analyses of technology, Latour claims that this approach will, if rigorously applied to analyses of technology in an actor-network perspective, reveal significant causalities and relationship.

Few, if any (not even Latour), have tried to develop this type of analysis further, however, a related, but much more diffuse attempt has been presented under the label of “technology as text”. In explaining the rationale for this, Keith Grint and Steve Woolgar write:

“..what a machine is, what it will do, what its effect will be, are the upshot of specific readings of the text rather than arising directly from the essence of an unmediated or self-explanatory technology. A technology’s capacity and capability is never transparently obvious and necessarily requires some form of interpretation; technology does not speak for itself but has to be spoken for” (Grint and Woolgar 1997, p. 32).

In justifying this, Grint and Woolgar calls “machine as text” a metaphor; they extend this by claiming that it may be convenient to treat the process of construction of a machine as “writing” and its use as “reading”, based on the axiomatic assumption that machines are interpretively flexible. However, they point out that “we have no wish to insist that machines *actually* are texts” (Grint and Woolgar 1997, p. 70 – emphasis by Grint and Woolgar) – just that they want to play against this metaphor, i.e. “..to see how far we can go with it”. They also want to explore this because they are dissatisfied with the implied causality in the cliché notion that technology creates social and cultural “impacts”, because they have a clear

¹⁵ This is a typical Latourian statement: “No matter how clever and crafted our novelists, they are no match for engineers” (Latour 1992, p. 248).

technological anti-determinist agenda. In adopting this approach, they seem to be following a fashionable trend in some quarters of social science that have adopted analytical approaches developed for analysis and interpretation of literature and mythology. However fertile this may be in literary discourses, employing this for analysis of technology is counterintuitive for a number of reasons: First of all, the analyst has to explain the meaning of the metaphors, i.e. translate this to plain language and terminology, as an introduction to this new conceptual universe. Secondly, they have to specify and delimit the validity of the meanings attributed to these concepts. Further, and more serious, these attempts estrange people who are interested in gaining insight into what experts on technology think about technology and its role in society and culture. Finally, by making this analytical detour, they violate the basic rule of research: Explanations should strive for simplicity and clarity. Not surprising, this approach, just as Latour's idea of using a linguistic approach, has not convinced other to adopt or develop this further.

Discussion

The two approaches reviewed above, i.e. the optimization theories and the social constructionist theories, are important because these hold a strong position, albeit in different communities. Whereas the optimization theories provide strong prescriptions on how technology should be designed and constructed, the social constructionist theories provide strong descriptions of how technology actually is created and adopted in society. However, both are weak in terms of explaining why. Thus, it would not be fertile to attempt analyzing the phenomenon of virtual keys as "text", even if accepting the possibility of a metaphorical approach because many aspects related to this are identified by metaphors (e.g. "keys"). In addition, the role of text (i.e. as plaintext and coded text) as symbols are important in virtual keys (e.g. cryptography), this would introduce at least two, possibly three indistinguishable levels of analysis, or in effect, equivocal. More important than the possibility of this confusion, an approach like this would disguise the relationship between technology, the systems that these are embedded in, and society. As implied by Winner's critique, one may claim that this approach neutralizes insights that an analysis may provide. For this reason, Latour's approach would be more interesting and possibly more successful, because using the ANT-approach, the links and relationships between all the elements that constitute a phenomenon are (in theory) made apparent. Still, transferring this to the case of virtual keys, in contrast to Latour's analysis of the Berlin keys, implies an increase in empirical and analytical complexity that makes this approach infeasible, in a way that carries resemblance to network theory in general: Even if analytically elegant, actually deploying these theories in empirical analysis proves to be very difficult because of the exponential increase in complexity as the number of elements in an analysis increase. Thus, it is really not possible to know how successful this type of approach would be – and what kind of insights this will provide.

Similar inadequacies are encountered in trying to apply other theoretical approaches to the analysis of virtual keys, even if these have their strengths and advantages. Thus, it is easy to imagine that one would encounter difficulties: Applying the “culture and process oriented theories” briefly described earlier would certainly provide interesting explanations on how engineering designers work and solve problems, but not why, the *raison d’etre* for these activities. This was the main reason for the shift in the project, i.e. that restricting the analysis of virtual keys to the laboratories would not explain important issues related to why the virtual keys emerge and the essential, external “design-parameters” that guide their work. Likewise, the aesthetic approach would give us interesting insights on the style and mode of articulation embedded in virtual keys. Even the evolutionary approach has a potential; an interesting analysis – which will be undertaken to some extent in a later chapter that analyzes continuity and discontinuity in keys – is, of course, what is really new with ICT, and in particular, what is new with virtual keys. Finally, the optimization theories, although strong on providing prescriptions, do this in spite of their weak foundation for this, because, they base these on ex-post insights, whereas the prescriptions are ex-ante. The relationship between ex-post and ex-ante is generally difficult, this is one reason why creating innovations is a challenge. However, optimization theories do not provide explanations of the type that is interesting in the inquiry of virtual key: What makes society adopt or require specific technological solutions, and how do designers interact with these in their work? Specifically, to the social constructionists, one may ask: Given the importance of social and cultural context in the shaping of technology, how does this actually guide and steer all the decisions made by engineers and designers? Furthermore, in the rapid development of ICT, how do the rigidities and tenaciousness of social systems actually intervene or constitute a dynamic for technological development? These questions and a host of others questions are difficult to answer following mainstream, current theories reviewed earlier, even if they provide numerous insights and illuminating explanations on parts of the aspects involved in designing and constructing ICT. In the following chapters, by focusing on the phenomenon of virtual keys, an attempt will be made to explore new ways of solving these difficulties.

3 Smart cards - the Janus of ICT?

In ancient Roman religion, Janus was the god who guarded and protected the entrance of a home. For this he was depicted having two faces in order to command a 360° view. He has also been depicted holding a key and a stick in his hands, i.e. a god who protected (stick) and controlled access (key). As a god of the entrance, he became associated with starts, beginnings, such as the early morning or the start of a year, as evident in the name “January” – and by extension, as an initiator and creator of innovations beneficial to society, such as speech, agriculture, architecture, i.e. Janus was the god of technological innovations. In contemporary, modern discourses, the term “Janus-face” is often invoked as a metaphor to depict controversies, situations where arguments and counterarguments confront each other in explanations of phenomenon, perhaps as a more sophisticated way of saying that there are at least two sides to a story; alluding to the two faces of Janus is also a way of showing ones knowledge of the classics. The Janus image is poignantly used as a comic strip in Bruno Latour’s *Science in action*, (Latour 1987, pp. 4, 32, 97, 141-143, 174). Latour initially uses the term Janus *bifrons*, bifrons being a rare term for *dimorphic*, which in botanical terminology means the unusual existence of two different forms of a species in a population, such as the leaves of a plant having two different forms.

Whereas Latour uses Janus as a vehicle for amplifying his unconventional, radical explanations of how science and technology evolves as a complex translation in which society and nature are intertwined (thus Janus), the focus in the following will be Janus as a symbol for the guardian and protector of ICT, involving the entrance to ICT and the key, or keys, and as the god of technological innovations. During the 1980s and 1990s, the evolution and diffusion of ICT has been dramatic and rapid in terms of societies becoming totally saturated with all kinds of communications and computer technologies and systems, such as mobile telephones, PCs, Internet, web, faxes (faxes are now becoming old-fashioned), etc. However, in other areas of ICT, the evolution and diffusion has been slow, disappointing adherents of “Moore’s law” who usually are confident in predicting rapid growth and diffusion of ICT-related innovations. This has particularly been in the domains which Janus rule, at the point of entrance to your home, if not your physical home (where you move your body in order to eat, sleep and rest), then your virtual home in term of your social and economic existence in a world which is becoming more and more “virtual”. This involves the ICT-effort of constructing electronic equivalents of institutions and mechanisms that are fundamental and important in “normal” society, in daily interaction, such as trust, protection, control, credibility and confidence. In the ICT-world this is broadly (and inaccurately) termed ICT security or other legalistically equivalent terminology. Trust, protection, credibility and confidence are elusive phenomenon, but still very basic to our existence. Just think of driving on a highway – if you did not trust other people driving there, and if you had to stop and scrutinize every passing car to make sure that you could trust them in not doing all the potential damage they may inflict when passing within the hitting range, then walking would be much more convenient and expedient.

Although numerous candidates and solutions exist in the ICT-world in terms of “ICT-security”, most notably in the widespread use of passwords, PIN-codes and cryptography for the “protection” and access, authorization, integrity of content of various actions mediated by ICT, others press forward in claiming to be much better than existing solutions. Of these, the most prominent is smart cards. One may even depict this as a movement, a large scale, apparently coordinated effort to promote the widespread diffusion and dissemination of the smart card technology. In 1999, this movement was given high political visibility in the European Union, as part for the *eEurope*-promotion. In a proclamation called the *Smart Card Charter* states that: “Smart cards empower people. They facilitate secure access to services and are a vital element in building trust and confidence.”¹⁶

Superficially, one may define smart card as an electronic key. However, this is superficial, because a smart card is much more, as the EU quote above indicates, with allusions to power, democracy, trust and confidence. Technically, smart cards may provide numerous applications by means of its potential for computing power and memory embedded in the integrated circuits of the card. The size and cost of smart cards, some claim, make smart cards an attractive and potent solution for ICT. However, this type of claim has been made for the past twenty years, ever since the first trails using smart cards on a large scale were made, first in France, initially as an electronic purse for petty cash transactions, such as payment for using public pay telephones (substitution for coins). A massive diffusion and development of the smart card was – and still is – envisaged to come if and when a few obstacles are removed.

Apart from one application, smart cards have never really made it. Simultaneously, as the diffusion of ICT increases, the concern over the lack of ICT-security is increasing. Many claim that in this, the Internet is most vulnerable, because it is notorious for its lack of security, making this medium a haven for hackers, virus-designers, embezzlers, organized crime, crackers, terrorists, spies, blackmailers, counterfeiters, pornographers, pedophiles, drug & weapon-dealers, any kind of imaginable evil, i.e. ICT stands the risk of being so compromised because of its lack of security that its potential may not be fully developed. The one success credited to smart cards is its use in telecommunications, in particular in the GSM mobile telephone system, where smart cards are known as SIM-cards, deriving its name from the term Subscriber Identity Module. Because it is called “SIM-card” and has a different size (much smaller) from the usual credit card size, few are aware that this is basically a smart card. The SIM-card makes it possible for a user of mobile telephone to use any mobile telephone set, its applications makes this the nervous system of the mobile telephone¹⁷. However, apart from SIM-cards and applications in satellite pay-TV and as prepaid public telephone card, the proliferation of smart cards has been slow.

¹⁶ Cf. <http://eeurope-smart-cards.org/sccv631.pdf> - p.2

¹⁷ One variety of SIM-cards are those which are sold with a prepaid amount of communication capacity, a type of card which is popular with teenagers (and their parents!) who want to have some economic restrictions on their mobile telephone expenses.

The manifest reason for this has been that magnetic stripe (“mag-stripes” in the industry jargon) cards have been more successful in terms of the most common applications related to payment – used as electronic debit or credit cards. In a technological perspective, the magnetic stripe cards are primitive, or “dumb” compared to smart cards because the former is a passive medium, the magnetic stripe’s capacity for storing information being limited. Because most of the information on the magnetic stripe is “open”, magnetic stripe cards may easily be copied or written over (manipulated), this being an important source to a lucrative counterfeit industry. Still, in terms of diffusion and use, the magnetic stripe card has been omnipotent – a quick look into any adult wallet will reveal a number of mag-stripe plastic cards¹⁸. According to industry insiders, the cost of smart cards – both the card itself, the costs of developing applications and the infrastructure, in particular the smart card readers – are so much higher than the magnetic stripe cards, that, in spite of their technological potential, smart cards have not yet been able to challenge the hegemony of magnetic stripe cards. In looking more closely at this question of costs of smart cards, the figures and aspirations varies greatly. Whereas some enthusiasts claim that smart cards will soon experience a breakthrough because the costs of a smart card has dropped during the past years¹⁹, others point to the high prize as a barrier, e.g., claiming that few customers are willing to pay Euro 29 for the smart card-based ID-card issued by Finland’s Population Register Center²⁰, i.e. approximately ten times more costly than the price quoted by the most optimistic. On the other hand, a major manufacturer and supplier of smart cards, in particular SIM-cards, as hardware, the French company Oberthur²¹ made a press release related to its financial results from 4Q in 2001, which explained that the company had experienced an increasing demand and subsequent growth in the shipment of banking smart cards, which balanced a downturn in the demand for SIM-cards from the mobile communications market. The increase in the demand for banking smart cards was explained in terms of sales of credit and debit smart cards to UK banks²², which are converting all their magnetic stripe cards to chip cards

¹⁸ Some of the cards may even be without a magnetic stripe, just a bar code – this being the “dumbest” variety.

¹⁹ Cf. article “Big Smart Card Growth Predicted for the US”, in the electronic journal Cardtechnology.com, January 2002, <http://www.ct-ctst.com/CT/> - states that the current prize of VISA smart cards is US\$ 1,65 (i.e. early 2002), compared with US\$ 3,50 two years ago.

²⁰ Cf. article “Finnish Agency Hopes to Recover from Slow Start with ID-card”, in the electronic journal Cardtechnology.com, January 2002, <http://www.ct-ctst.com/CT/> -

²¹ Cf. <http://www.oberthur.com>

²² Cf. article “Oberthur Hits Revised Growth Estimates Despite SIM Slump” - in the electronic journal Cardtechnology.com, January 2002, <http://www.ct-ctst.com/CT/> - Oberthur, officially known as Groupe Francois-Charles Oberthur, with HQ in Paris, is a fascinating company because it claims to be the world’s largest printer of postal stamps and the third largest printer of bank notes, lottery scratching tickets, etc – what they term “..to print secure, high-technology products”, cf. <http://www.oberthur.com>.

(i.e. smart cards) that comply with international EMV-standards²³. In addition to this news, other major institutions made policy decisions during 2001, to evolve from magnetic stripe to smart cards during the next years – this may indicate a gradual adoption of smart cards in the banking sectors as debit and credit cards, and as an electronic ID-card for various governmental agencies. Some of these cards contain applications that will enable digital signature, i.e. software for encrypting messages and authentication of the user. Still, this optimistic impression conveyed by the smart card industry of an imminent “breakthrough” is old, it reflects a sentiment of hope as to a profitable future for the technological solutions in which they have invested much into. In many ways, this is understandable and rational, because smart cards are in many ways technologically ingenious. In the next pages, a short technological tour will be made in order to explain this.

Smart card technology

The term “smart card” is a generic, somewhat colloquial term for a type of plastic card in which a microprocessor or a memory chip is embedded. However, there are several varieties of smart cards, as will be explained shortly. What may be termed ordinary smart cards have a size and thickness identical to credit cards²⁴. Due to the embedded microprocessor chip, which is technically identical to processors in some personal computers, the card has been given the name “smart” in English and most other European languages, because the processor has a capability of processing information in the way information is defined in computer science. However, in French, smart cards are called “cartes à puce”, puce meaning louse, for which reason this could be translated as “bug card” or “lice card”. In the early days of the smart cards, in the early 1980s, smart card enthusiasts were fond of telling audiences “This card is a computer!” while flickering a smart card between their fingers.

Smart cards may be differentiated in terms of their physical interface to the outside world, and in terms of the technology embedded in the cards. In terms of the physical interface, distinction is made between:

- contact smart cards (most common), and
- contactless smart card.

In terms of embedded technology, distinction is made between cards that only contain a memory chip, for which reason they are called memory cards, as a contrast to microprocessor cards, or what is sometimes called ICC, an acronym for integrated circuit card. When industry insiders use the term smart card, they usually mean a contact card with an embedded

²³ EMV-standard = Europay, Mastercard and VISA-standard was developed in 1995 by the three companies for smart cards. According to one source, “The EMV-specification ensures that all Europay, Mastercard and VISA-branded smart cards will operate with all chip-reading devices, regardless of location, financial institution or manufacturers. “ – cf. <http://www.oasis-technology.com/products/emv>.

²⁴ A new, low-cost smart card that was launched on the markets in October 2001 was somewhat thinner than the ordinary plastic type because it was made of paper, but its height and width was identical to the “normal” credit card.

microprocessor, i.e. this is the “default” definition of a smart card, a term which also will be adopted in this work also for reasons of convenience.

Contact smart cards (the “real” smart cards) become operational when they are inserted in a slit-like socket in a special reader, which specialists call a CAD (Card Acceptance Device). The socket in the CAD has pins that connect to contact pads on the smart card, and by this the microprocessor or the memory chip on the card is activated and becomes capable of communication to the outside world, usually through a host machine, such as a mobile telephone, a POS-terminal, a PC, etc. Smart cards that are called contactless (which sounds strange to the uninitiated) communicate to the outside world by means of short-range radio waves, i.e. propagation inside a range of less than one meter. This requires a different type of CAD compared to the contact smart cards, because it has to have a radio capability in order to communicate with the smart card. In the contactless smart card, a miniature radio antenna is embedded in the vicinity of the microprocessor and the card receives its electrical power supply from a small battery, also embedded in the card. The contact smart card, in contrast, is powered by electricity supplied from the CAD, through the pins dedicated to this function in the socket.

The other dimensions that differentiate smart cards are types of technology embedded in the card. Of these, there are basically two types:

- Cards in which a *memory chip* is embedded, for which reason their main field of application has been as prepaid telephone cards, used as electronic tokens instead of coins. When the prepaid amount is used up, the cards become invalid or worthless, save as a collector’s item (some of the earliest memory smart cards are now traded for thousands of dollars). Some terminological purists feel that these types of cards should not be called smart cards; the term “smart” is misleading because memory cards lack computational capability.
- Cards in which a *microprocessor* is embedded, i.e. the “real” smart card, or what some prefer to call ICC – integrated circuit card. In mobile telephones of the GSM-system, the smart card used is better known by the acronymic of its application, SIM, which means “Subscriber Identity Module”. Having the size of a small stamp, most people think of the SIM-card as something unique to the mobile telephone, but the reason for this size is that the SIM-cards have been stripped of a lot of plastic in order to fit into slim mobile telephone handsets. Thus the plastic “casing” in which the microprocessor of the SIM-card is embedded is minimal compared to the ordinary credit card size. Nevertheless, this is a “real” contact smart card.

“ISO 7816” is the designation of the technical standard that defines the contact smart card – ISO meaning the International Standardization Organization, which is formally a NGO consisting of 130 member countries, with headquarters in Geneva, Switzerland. The various standards agreed upon in ISO are given a number, thus ISO 7816 is the identity of the contact smart card standard; its full name is “Integrated Circuit Cards with Electrical Contacts”. The contactless smart card is defined in the standard named ISO 14443. The first version of ISO 7816 was established in 1987, and by this it became an international standard. In becoming an

international standard, a technological solution becomes defined with a permanence which is usually significant, an aspect which will be explored further later.

The ISO 7816 is a typical horizontal standard, thus one may also call ISO 7816 a general standard. In contrast, vertical standards, or industrial standards, determine standards for specific purposes or applications, within and in compliance with, the requirements of the horizontal, or general, standard. A characteristic of the smart card world during the past decade is the creation of a multitude of vertical standards. This reflects the variety and complexity of real, planned and potential applications and uses of smart cards. The status of vertical standards will shortly be elucidated, however, this situation may explain the numerous efforts to harmonize smart cards, as evident in the eEurope initiative, as many perceive this as a major obstacle for the mass diffusion of smart cards.

The ISO 7816 standard now consists of eleven parts. The first parts, or the bottom layers of the standard define the physical aspects of the smart card, while the top layers deal with applications, content and interoperability. Thus parts 1 to 3 of the ISO 7816 define the basic characteristics of a contact smart card in terms of its hardware, i.e. material, size and shape of the card itself, the size and positions of the contact pads and the electronic components (e.g. the microprocessor), and the electrical signals and transmission protocols to be used in the electronic components. The different parts of the ISO 7816 are as follows:

- Part 1: Physical characteristics
- Part 2: Dimension and location of contacts
- Part 3: Electronic signals and transmission protocol
- Part 4: Inter-industry commands and responses
- Part 5: Numbering system and registration system for application identifiers²⁵
- Part 6: Inter-industry data elements
- Part 7: Inter-industry commands for Structured Card Query Language
- Part 8: Security related to inter-industry commands
- Part 9: Additional inter-industry commands and security attributes
- Part 10: Electronic signals and answer to reset for synchronous cards
- Part 11: Personal verification through biometric methods.

Although ISO 7816 has been revised several times after 1987, one may claim that by 2002, the basic design of the contact smart card has become stable, i.e. it is governed by a *dominant design* (cf. Abernathy and Clark 1985; Utterbach and Suarez 1993). A change of the basic design would demand a complex, lengthy and highly political process. For this reason, the main threat to the stability of its present design may be that the smart card technology becomes obsolete, or that other technological solutions serve the applications better, i.e. that the technology in the future may be abandoned. However, at present, this does not seem to be a realistic scenario. Even if the basic design of the smart card may be characterized as stable

²⁵ The Copenhagen Telephone Company, or better known as KTAS by Danes, is now the registration authority according to ISO 7816-5. At the charge of US\$ 500, the KTAS will, with the recommendation of your national ISO-body, register the application and give this a unique identifier.

and locked-in, this is not total. As evident by the numerous vertical standards that compete within the boundaries of the ISO 7816 as a horizontal standard, there may be maneuverability or a space for interpretation that may give technological designers some degrees of freedom. This aspect will be explained further below, however, first a close look at the smart card as a piece of hardware.

In the ISO 7816, part 1, the size of a smart card is defined as 85,6 millimetres in width, 53,98 millimetres in height, with a thickness of 0,78 millimetre. The standard does not state that the card has to be made of plastic, however, it specifies numerous physical characteristics that a card has to comply to, such as the maximum tolerance of bending a card before it breaks, its tolerance of exposure to ultraviolet radiation, etc. The positions of the contact pads on the card are specified in part 2 of the standard. Figure 1 is a close-up of the interface, or contact pads of the smart card²⁶.

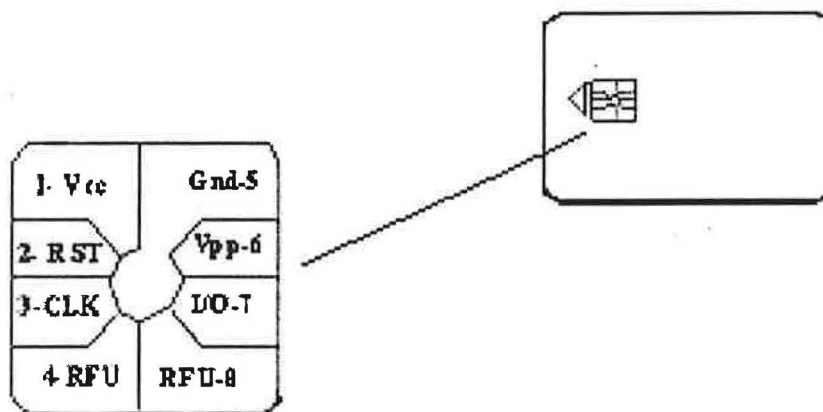


Figure 3.1: The contact pads (enlarged view) of a smart card and location on a standard credit cards sized plastic card.

When a smart card is inserted into a CAD (card reader), the contact pads are connected to pins inside the reader, one pin for each pad on the smart card. The ISO 7816 part 2 has defined eight pads, or what is called “pin assignments” with numbers and names to identify, and determine what kind of function these pads have:

- C1 or Vcc – which supplies electrical power to the chip, either 3 volt or 5 volt (low voltage)
- C2 or RST – the latter being an abbreviation for “reset”, a function which resets the microprocessor in the smart card,

²⁶ Source: <http://www.scia.org/knowledgebase/default.htm>

- C3 or CLK – the latter being an abbreviation for “clock”, which supplies the microprocessor in the smart card with clock signal, because smart cards do not have their own, internal clock generation, such as in PCs or ordinary computers.
- C4 or RFU – the latter being an abbreviation for “reserved for future use” – in 2002, there are no standards defining what this may be.
- C5 or Gnd – the latter being an abbreviation for “ground” – i.e. the reference voltage which should usually be 0 volts (no current).
- C6 or Vpp – the latter being an abbreviation for “programming voltage point”, which is not used any more, but was used in the early smart cards for supplying programming voltage to the EEPROM (electrically erasable programmable read-only memory).
- C7 or I/O – the latter being an abbreviation for “input/output” – this being the point at which data and commands are communicated, between the smart card and the outside world.
- C8 or RFU – identical with C4, i.e. “reserved for future use”, but not yet (in 2002) in use.

In order to function as a smart card, the card must, as a minimum, comply with the requirements set for C7 and C5 – the other pads are optional, of which C4 and C8 have not yet been assigned any function.

As stated earlier, the ISO 7816 part 3 defines the electrical characteristics of a smart card, i.e. the electronic signals and the transmission protocols (rules) of the smart card. This is very detailed in terms of how the various parameters should be set, as illustrated by how the standard defines “Reset of the card”:

“A card with an active low reset is reset by maintaining RST in state L for at least 40 000 clock cycles (t_3) after the clock signal is applied on CLK (time t_3 after T_0). Thus if no Answer to Reset begins within 40 000 clock cycles (t_3) with RST in state L, RST is put to state H (at time T_1). The Answer to Reset on I/O shall begin between 400 and 40 000 clock cycles (t_1) after the rising edge of the signal on RST (time t_1 after T_1).”²⁷

Thus, in terms of hardware and the physical properties of a smart card, the big issues were resolved and “frozen”, i.e. given permanence as expressed by the standard, which was agreed upon in 1987, under the aegis of ISO.

The establishment of a standard in ISO, the International Standardization Organization, marks the end of a lengthy, usually laborious process involving many serious men (usually senior engineers) organized in a hierarchy of technical committees, sub-committees, working groups, task-forces, etc. Although the agenda in these types of work are strictly technical, most analysts and participants are unanimous in that these processes are highly political, because the shaping of standards involve matters that may be vital for the economic future of a country or a company. Becoming a dominant design implies that the technology has become “locked-in” – the specifics defined in the ISO 7816 are so compelling that attempting to enter the smart card market using a different design would be unfeasible for

²⁷ Cf.: <http://www.scia.org/knowledgebase/default.htm>

numerous reasons. However, whereas the hardware aspects of smart cards are ruled by the rigidities of a dominant design, this is not the case with the information and applications contained in the microprocessor, i.e. the content of the smart card. This is the domain of the vertical standards, or what is also called “industry specifications”. These may be created by companies, often as they cooperate in consortia or in joint projects. In the smart card industry, the most prominent among these (apart from the SIM-card standard) is the EMV-standard, which has derived its name from the cooperating companies Europay, MasterCard and VISA – an alliance representing the largest international organizations in the credit card business. This, and company specific implementations (interpretations) of the EMV-standard, competes with the Mondex-system, which is an electronic cash system developed by MasterCard, as a proprietary system. Similarly, Europay has led a standardization effort that resulted in the CEPS-standard, which is an abbreviation for “Common Electronic Purse Specification”. In addition to these, Microsoft has taken leadership of a standardization effort called PC/SC, which is short for “Personal Computer/Smart Card”. As one may guess, the intention of this is to make a standard for smart cards for use in PCs and workstations. As evident in an overview article²⁸ written by the US consultancy firm Mobile-Mind Inc., there is at present a jungle of industrial standards and standards creation initiatives at various stages, such as:

- The SET (Secure Electronic Transactions) specifications for cryptography, which include descriptions of the smart cards they use to perform SET transactions.
- RSA, also a cryptographic system and organization, which has published a file hierarchy and data description for accessing PKI certificates and associated information on cryptographic tokens including smart cards.
- Visa has published specifications for Visa Cash, the Visa Integrated Circuit Card.
- GlobalPlatform is a consortium organized by Visa which is drawing up a specification based on Visa Open Platform for loading applications on and deleting applications from multi-application smart cards.
- MasterCard has formed the Global Mobile Commerce Team and the Chip Vendor Services Program.
- American Express has formed The Interoperability Consortium, for developing smart card applications.
- The Java Card Forum and JavaSoft have developed software and maintain specifications for the Java Card, a type of smart card.
- The OpenCard Framework is an initiative taken for specifications related to a method for accessing smart cards from the Java programming language.
- The Small Terminal Interoperability Platform consortium is undertaking a similar effort.
- The Radicchio, based on Global Mobile Commerce Forum, is studying the use of PKI smart cards on wireless networks.

²⁸ Cf. <http://www.mobile-mind.com/scstd.htm>

- The Mobile Electronic Signature Consortium is writing a specification for wireless e-commerce.
- The PKI Forum is also writing specifications for digital signatures.
- MasterCard is also starting a coalition to draft U.S. digital ID procedures for issuing, revoking and establishing digital user identifications. The coalition includes ACI Worldwide, Gemplus, Bull Smart Cards & Terminals Giesecke & Devrient; Schlumberger and Unisys.
- The Mobey Forum is a collection of banks, mobile handset manufacturers and smart card manufacturers who are trying develop alternative standards to the hegemony of telecom operators in the SIM-cards domain, this by keeping them out of this work.
- The ETSI²⁹ Technical Committee Security has also developed a standard for the format of PKI certificates, ES 201 733. The SIM-card version of the contact smart card is standardized in a separate standard in terms of its functions and applications (the ETSI-standards GSM 11.11 and 11.14).
- The World Airline Entertainment Association has put out a specification for the use of smart cards by passengers in airplanes.
- The International Air Transport Association sells a specification for smart cards in travel and entertainment cards.
- The SIMalliance is writing specifications for protocols to connect GSM SIM cards to the Internet. Their approach to this work is to redesign the existing WAP protocols.
- The Smart Card Constituency working under the banner of eEurope is proposing to write a set of smart card interoperability specifications, based on the work of numerous “trail-blazers”. One of these in connecting to the Japanese “Next generation IC Card System Study Group”, which is planning a large-scale introduction of smart cards in Japan.
- The Card Application Management System Consortium consists of just Visa and MasterCard.
- Israel has a standard concerning the use of Hebrew for textual data in smart cards.

A brief history of smart cards

In 1967, a patent, filed in USA by the inventor Jules K. Ellingsboe, described a credit card with an embedded microprocessor, which subsequently became US patent no. 3.637.994. However, according to one source³⁰, it is not obvious that Ellingsboe was the first inventor, as two German engineers, Jurgen Dethloff and Helmut Grötrupp announced a similar invention, also in 1967. A few years later, a Japanese inventor, Kunitaka Arimura, successfully filed for a Japanese patent for a device that was essentially a smart card, and in May 1971, Paul

²⁹ ETSI is an acronym for the European Telecommunications Standardization Institute, which is based Sophia Antipolis, in the beautiful hills above Antibes, next to Nice in France.

³⁰ Cf. <http://www.mobile-mind.com/htm/scstd.htm>

Castrucci of IBM obtained a US patent for an invention called “Information Card”, this also being essentially a smart card. Ellingsboe’s invention from 1967 was probably the first smart card, however, almost twenty years of development ensued until the smart card became standardized as ISO 7816. The two decades in-between may be characterized as an intense developmental phase, or stage, in which numerous patents were filed related to various aspects of smart card technology, in particular in the 1970s. Roland Moreno, who originally was a journalist in France, filed 47 patents related to smart cards during the period 1974-79. A typical technology entrepreneur, he simultaneously founded a company, Innovatron, based in Paris, for the purpose of developing smart cards, and this company is still (2002) in the business.

As the smart card evolved during the 1970s, the big players in the electronic equipment manufacturing industry became involved in its development. The interest in smart cards was initially greatest in Europe, in particular in France, which may explain the dominance of European companies in the subsequent growth of a smart card industry. Thus, the leadership in smart card development was taken by French companies, in particular CII-Honeywell-BULL³¹, Schlumberger and, what is now known as Telecom France³², were strong promoters of smart card technology and related applications. At CII-Honeywell-BULL, the engineer and inventor Michel Ugon was very active, as Ugon and his team filed over 1200 patents related to smart cards. Telecom France was active as organizers of large trails in which smart cards were tested, such as the trails at Velizy outside Paris, in which smart cards were used for pay-TV, and the commercial introduction of the “Telecarte” in 1983, the prepaid memory card for use in public pay telephones. Simultaneously, other large scale trails were carried out in France: In the period of 1982 to 1984, French banks, in collaboration with smart card manufacturers, distributed 125.000 smart cards and 650 smart card reader terminals in trails that attracted much attention, also from outside France.³³ In fact, inspired by this, the Norwegian Telecommunications Research Establishment in 1983 launched a trail in Lillestrøm, a small town near Oslo, using CII-Honeywell-BULL smart cards, in cooperation with local banks and a few shops. In addition, a few public pay telephones in Lillestrøm were installed with card readers for “Telecartes”. During the 1980s, the development of the smart cards were characterized by three trends:

³¹ This company has changed its official name often; it now calls itself Group Bull. The name “Bull” came from Fredrik Rosen Bull (1882-1925), an inventor who lived most of his life in Oslo. He died at the age of 43 from cancer. He developed and patented technology for punch card equipment, in particular for insurance companies. This technology constituted the core of a company established with a companion, K. A. Knutsen, who immigrated to France in 1930. Thus, the name “Bull” became a French company name.

³² Telecom France was at that time (1970s) known as “DGT”, or more officially as “Direction General des Telecommunications”, which during the late 1970s and early 1980s was well known for being technologically avant garde because of its promotion of “Minitel” (videotex), the Transpac communication network based on packets switching, digital telephony, etc.

³³ Cf. M. Ugon, “L’odyssée de la carte à puce”, article in <http://f1my/axtcp/cartapuc.htm>

- The processing and memory capability of the integrated circuits in the card increased and improved rapidly during this initial development phase, particularly as developers successfully adapted CMOS-technology³⁴ for use in smart cards, this subsequently becoming the dominant technological solution for smart card.
- In the GSM-development, which took place in parallel during the first part of the 1980s, the smart card became part of the system's technological solution as the subscriber identity modul, or more well-known as the SIM-card. In particular, the SIM-card was assigned two critical applications: Encrypting the signals for the digital radio signal code, and for the authorization and authentication applications of the subscriber, the latter essentially by means of the PIN-code for switching on the mobile telephone set. Thus, the smart card was adapted to the GSM-system for ensuring security and secrecy. This became feasible as the processing capability, in particular the execution speed, of the smart card's microprocessor increased. However, according to people who participated in the development of GSM, the idea of "plastic roaming" was also a reason for choosing a smart card solution in GSM: At that time, in the early 1980s, they anticipated that the cost of a GSM mobile handset would be so high that sharing of this would be attractive. Thus, by separating the subscription of GSM (which would be embedded in the smart card) from the ownership of the handset, two or more people could share a handset. An application similar to the SIM-card was adapted for set-up boxes in pay-TV, for decoding satellite broadcasted signals. The rapid growth and diffusion of GSM contributed significantly to the initial diffusion of smart cards.
- Apart from the SIM-card, the main application of the smart card has been as a memory card, used as a prepaid "electronic wallet" for all kinds of vending machines, which some characterize as not being a real smart card. However, this application has been popular with telephone operating companies, for their public pay-telephones, as public pay-telephones are exposed to much damage and vandalism caused by thieves trying to steal coins. An additional advantage is lower management costs related to handling coins. In Denmark, the Danmønt prepaid petty cash electronic smart card may also be used for a variety of vending machines, such as buying tickets for bus and subways, etc. In the concept of "campus cards", universities often issue these types of cards to students for using copy machines, in addition to being electronic keys.

Thus, until the latter part of the 1990s, the diffusion and proliferation of smart cards were mainly in telecommunications related applications, of which the SIM-card used in GSM mobile communication handsets was the largest. The use of smart cards in the banking sector, as credit or debit card, which many thought would be the "killer-app" of smart cards in the initial years of the smart card development, has not been large, except in France. However, as the new millennia began, there are visible signs that the diffusion of smart cards is going to

³⁴ CMOS = complementary metal oxide semiconductors. CMOS is attractive because it requires less electrical power to run, compared with other types of integrated circuits, thus CMOS-technology is much used in portable electronic devices.

increase, as numerous reports indicate a significantly increased demand for smart cards. In spite of these indications, the picture is not very clear, as facts are in conflict. For the moment, this topic will be left, for the benefit of exploring an important aspect related to the development of smart card, i.e. the history of keys and locks – and the question of what is really new with these, compared to the old keys and locks, i.e. the question of continuity and discontinuity in the development of locks and keys.

4 Continuity and discontinuity in locks and keys

Introduction: How novel are innovations?

What is really new with electronic keys and locks? At a fundamental level, this type of question addresses issues related to continuity and discontinuity in technological development. However, it also involves how technology is perceived and understood - and explained. In explanations that emphasize continuity, the focus is set on how various elements and functions of the claimed innovation are related to earlier technological solutions and decisions, i.e. that technological development may be explained in terms of accumulation of countless, small technical adjustments of technology that have existed earlier, each small step forward based on minor modifications of previous technological solutions³⁵. Thus, a long, evolutionary chain of technological solutions emerge, such as seen in some discourses that claim that the fundamentals of modern digital communication emerged in antiquity, because in ancient Rome and Greece, semaphores were used, based on reflecting sunrays in mirrors and using special signals to convey a message. These in turn may be based on even older precedents and antecedents - even these ancient semaphores were not really so novel because ancient, primitive societies are known to have used simple communication technologies, as evident in use of the jungle drum (Africa), whistling (Canary islands), smoke and fire. In the context of electronic locks and keys, the question of continuity is relevant because one may rightfully claim that these new technologies merely represent a *substitution* of technological solutions that have existed for a long time: As the purpose of having locks and keys remain unchanged, new types of locks and keys merely represent a technological up-grading, i.e. a relatively minor adjustment of old technologies – the “new” technologies are functionally equivalent to the old. For this reason, those who favour explanations of technological development as continuous would claim that the new keys and locks are not very different from the old; their development fit nicely into an evolutionary trajectory. In contrast to this, advocates of discontinuity would claim that although electronic keys and locks may have some functional similarities and employ metaphorical terms derived from physical locks and

³⁵ A related, but different type of explanation is that new technologies achieve aims similar to the old technologies, however, this is done by a detour using new technology, creating an illusion of increased efficiency and novelty, i.e. innovation. This type of explanation may be encountered in academic communities, among senior academics who have experienced the transition from old mechanical typewriters to PCs. The claim made is that PCs have not improved the efficiency and quality of academic writing. On the contrary, the new electronic tools have only increased the outpour of meaningless texts and consumption of paper for various drafts printed out uncritically: The focus and conciseness of the old style of working has been lost, simultaneously the secretary who did the typing in the old days, has disappeared – so academics now spend more time doing things they are not good at, out of focus, pressing buttons that spew out verbose text that (admittedly) is graphically good, but in terms of content, represents no improvement or change from the old days.

keys, these similarities are superficial, because the “new” locks and keys differ significantly from anything that have existed previously. For this reason, their emergences represent a technological discontinuity.

In innovation theories, the idea of technological discontinuities as a contrast to continuity in explaining technological development is disputed. In the former, the focus is set on identifying what is new and distinct from the old, and in the judgement of this, the degree and inherent aspects of the novelties are characterized. Thus, both continuities and discontinuities are recognized, as evident in the various dichotomies, such as the terms “radical” vs. “incremental” innovations, and that radical innovations are often associated with shifts in techno-economic paradigm (Freeman and Perez 1988). However, when the burden of proof is put on innovation theorist in discussions with those who advocate continuity, the former will claim that something new qualifies as an innovation because this has not existed previously – they may even employ evolutionary terminology in that an innovation is analogue to a new specie: Even if a new specie consist of elements or functional analogues that existed previously, it is still novel because it has not existed before. This point may be illustrated³⁶: No matter how many horses and diligences are chained together, and no matter how ingeniously this is undertaken, these are very different from railroad-cars pulled by steam engine locomotives, in spite of clear antecedents and technical precedents in diligences pulled by horses and in spite of functional similarities (transportation). However, in dealing with locks and keys, this question is very complex because in terms of technology, social institutions that govern these and the metaphors employed, the distinctions are subtle, perhaps indistinguishable. Thus, the question of predecessors and technological antecedents needs to be discussed. In this, one may distinguish at least three different strategies of explanations, of which two will be presented briefly first, because in this chapter, the main emphasis will be put on the third.

First, as technological innovations diffuse and become "naturalized", i.e. become integrated and adopted in society, they simultaneously undergo a metamorphosis, which may be termed *trivialization*³⁷, or, alternately, *domestication* (Goody 1977, cf. Lie and Sørensen

³⁶ This illustration was presented by Esben Slot-Andersen in his oral Ph. D. defence, in early spring 1994 at the University of Roskilde and attributed to Joseph Schumpeter. Schumpeter's authorship is voluminous – I have failed to find this point in his writings, which does not really matter, because the point is succinct.

³⁷ This may also be termed the "Colombus-egg-syndrome", alluding to the story of an intermezzo between Christopher Columbus and his patron, the Spanish queen Isabella I (1451-1504). According to the tale, during a dinner party celebrating the return of Columbus and the discovery of America (or India, which was the initial belief), the queen made a comment that the discovery of America must have been easy because Columbus had just kept a steady course sailing westward, i.e. belittling the feat Columbus has undertaken. In response to this, Columbus asked the queen if she could make a boiled egg (part of the meal served) stand on its end. The queen attempted this a few times, but each time the egg rolled over sideways. Whereupon Columbus took the egg and hit it firmly on the table, making it stand on the end because he had crushed part of the eggshell flat. According to the tale, Columbus turned to the queen and said: 'This too was easy, but nobody had thought about it before'. However, this tale is disputed as others attribute this solution to the Italian renaissance architect Filippo Brunelleschi (1377-1446), the architect of the famous dome of the cathedral in Florence, Italy.

1996) for an elaboration of this concept in technology analysis). In a diffusion process, knowledge of the new technological device or process will increase as the society start to learn how and why it works – diffusion is simultaneously a familiarization process. As the innovation becomes integrated into the socio-technical landscape of society, it becomes taken for granted, i.e. the diffusion process is pervasive, the technological innovation becomes "seamlessly" integrated in society (cf. Law and Bijker 1992). Now, in year 2002, most people will take for granted that shops accept electronic payment for purchases by means of a plastic card; it is as trivial as a piece of bread or a potato. If and when electronic payment fails (e.g. a computer network shut-down, the PIN-code is forgotten, etc.), a crisis of payment will instantly emerge. Anything that is taken for granted, such as air, water, bicycles, mobile telephones or TV, are simultaneously trivial if they function and look as expected. The related term *domestication* of technology implies the same type of integration, however, the term carries a connotation of a power-relationship, i.e. the technology has been tamed to serve its users, just as wild animals and plants in ancient times were tamed and integrated into the subsistence economy of our ancestors. However, as trivialization ensues, the novelty of an innovation wanes, this may explain why the continuity to the past becomes important.

Secondly, judgement of what is new often depend who makes the judgement, what kind of knowledge, perspective and relationship they have to the technology. The phenomenon of *black-box* is closely related to this. As a concept, which originated in cybernetics in order to represent and focus on the external relationship of a system (system=black-box), it depicts that in the ordinary use of a technology, users will judge the novelty in terms of its interface and functionality, or effects, i.e. the external relationship of the technological solution. Thus, to an ordinary telephone user or a television viewer, the distinction of analogue and digital technology is ordinarily not significant – he or she could not care less, as long as it works (functionality) as expected and looks familiar (interface and outward physical shape or styling). Thus, most modern people will feel intimate and even identify themselves with mobile telephones, however, few understand (and care to understand) why it works and what the different components, software, etc inside the mobile telephone actually do. The transition from analogue to digital technology, which caused radical changes in terms of technology, economic and organizational structures in the telecommunication sector – is an impregnable black-box to ordinary users because their relationship to telecommunications, such as telephone, has not changed, or changed only moderately as the interface on telephone sets have been modernized, e.g. introduction of touch-button dials substituting the old number dials, slightly higher quality of sound, etc.³⁸ Even Internet, which most felt as a radical novelty when this was initially introduced, now seems trivial because it has become black-boxed – the technological system which delivers all the messages is a black-box which now delivers almost the same type of written messages as done by the old style postal system; even if the speed and quality is different, this is

³⁸ An interesting contrast to this is the preoccupation with battery technology – this probably because of the frustrations caused by batteries running out of power during an intense and interesting telephone conversation.

conceptually similar to the content that the ancient postal system delivered in one's mailbox. This is amplified by the use of postal metaphors and icons in most electronic mail systems (however, the stamp and licking associated with this is absent).

In the third approach, those who focus on continuity in an evolutionary perspective on technological development will claim that most changes in technology are minor, gradual, based on moderate modifications of existing technology. In this, the idea of technological discontinuities, or radical innovations, is antithetical because they will claim that in development of novelties, precedents and technological antecedents are strong. Thus, nothing new will emerge out of a void; novelties are created because these, more often than not, are based on models or solutions that have already been developed. Thus, in technology, just as in nature, development is gradual and continuous; to the extent novelties are created, these are based on modifications or recombination of elements that already exist, or by transferring existing solutions to new applications or material, i.e. that antecedents and technological predecessors are important. Georg Basalla, an advocate of this approach, points to numerous cases, such as the barbed wire, which is based on copying thorny twigs, or hang-gliders, which are clearly inspired by birds (Basalla 1988). In elaborating this, he writes that: "Functional requirements have always had a strong influence on choice of an appropriate antecedent and because functionality may well cut across established technological boundary lines, the antecedent may not always be the one that appears initially to be the most obvious one" (Basalla 1988, p. 62-63).

According to the evolutionary approach to technological development, the idea of outstanding novelty, as implied by the term "radical innovation", may be attributed to a Western cultural ideal for technological heroes and dramatization, typical of 19th century society (Basalla, p 59). The institution of patents and patent protection, according to Basalla, "...bestows societal recognition on an inventor and distorts the extent of the debt owed to the past by encouraging the concealment of the network of ties that lead from earlier, related artefacts." (Basalla 1988, p. 61). Thus Basalla claims that innovation theory confuses socio-economic and political impacts of technology with inherent properties of the technology itself. The former, the impacts, are evident in the type of terminology which is used and associated with technological development, such as the "Industrial Revolution", thus making connotations to historical-political terms such as the "French Revolution" (1787). Elaborating this, Basalla claims that:

"The industrial changes of the late eighteenth and early nineteenth centuries were truly revolutionary in the ways they affected the lives and fortunes of the people of Great Britain. Yet the machines, the steam engines that powered them, were the outcome of evolutionary changes within technology. Neither marked an abrupt break with the past. The economic and social consequences of these developments, on the other hand, were so far-reaching that they transformed the social order." (Basalla 1988, p. 61).

Still, even if these arguments are accepted, even Basalla does not deny the phenomenon of novelty – that something new constitutes the dynamic and essential core of technological development. Furthermore, these novelties are not results of accidents, more often than not they are created as the result of ideas that humans conceive. These may be explained as the

result of a broad range of sources, ranging from dreams and fantasies in the minds of creative personalities at one extreme, to necessities created by economic or political reasons. Thus, as evident in other technological evolutionary theorists such as Sahal (Sahal 1985), instead of denying the possibility of extraordinary novelties, one may, as a parallel to nature, accept that at certain points in the evolution of earth, some species developed the capability to fly (birds), while others developed the capability of speech, both of which are distinctly novel, representing a demarcation to other species and point of departure for autonomous developmental trajectories.

As Joel Mokyr (1990) has pointed out in his analysis of evolution in terms of explaining technological change, modern bio-evolutionary theories do not exclude the possibility of sudden and radical changes occurring in a short period of time, i.e. “..chaotic bifurcations and catastrophes leading to unpredictable new steady states” (p. 273). Secondly, one should also distinguish two different meanings of the term evolution; one that equates evolution with gradual change and continuous development, and one that focuses on explaining change, specifically the mechanisms of selection and mutation. Furthermore, in reflecting on why evolutionary theoretical analogies has an appeal in explaining social and cultural change, Mokyr makes (p. 275) a distinction between two approaches:

- a *heuristic approach*, i.e. a successful explanatory strategy of one phenomenon is transferred to a new area in which explanations are unsatisfactory, in search or attempt of new explanations,
- a *sylogistic approach*, because a theory has had success in explaining one phenomenon, it may also successfully explain other areas, i.e. what Mokyr calls “analogy-as-justification”.

Mokyr adopts an approach to technological evolution in which his central unit of analysis is “technique”, which he defines as “knowledge of how to produce goods or service in a specific way – are analogous of species, and that changes in them have evolutionary character” (p. 275). Although Basalla (1988, p. 2-3) warns the reader of the dangers of using analogies of evolution in explanations of technological development, his basic unit of analysis is the technological artefact, i.e. the physical, artificial, human-made object, i.e. apparently a more concrete understanding of technology compared with Mokyr’s notion of “technique”. Whereas Basalla emphasizes the gradual development of technology as a parallel to his understanding of biological evolution, in Mokyr’s approach, the possibility of sudden changes, discontinuities are present. Thus Mokyr states that “..path-dependency in biological evolution is much stronger than in technological progress” (p. 285).

Turing now electronic locks and keys, the questions raised above are not resolved easily and should be analysed carefully. Clearly, there are strong precedents and technological antecedents to the modern lock and keys, as will be explained in the following, in the histories of these technologies. Still, there are aspects with these technologies that represent discontinuities. These discontinuities in turn may explain the diffusion pattern of modern, electronic keys and locks, in particular the role of smart cards, or why chip-card technology so far has not had the expected success. Following an evolutionary technological analytical

strategy, is this due to aspects outside the technology itself, or is it due to the technology? Is smart card technology a technology in search of something to solve? The answer to this is not obvious, as will be evident in this and the following chapters.

A brief history of keys

Keys, and the locks these open or close, are distinct as a category of technology because they are primarily designed in order to *regulate* the behaviours of fellow humans. The effect of these design criteria is social discrimination, because those who possess a key (in contrast to non-possession) have rights of access that are denied to those not having a key. The ancestry of locks and keys may be traced to the rise of civilizations, i.e. to the emergence of societies with high population densities, in contrast to less organized and stratified societies, such as tribes or bands of hunters-gatherers, in which the use of lock and keys historically has been rare. The obvious, trivial feature of locks are that they are designed to control what is considered valuables, thus they represent technical solutions to the maintenance and management of ownership, in whatever way this is socially defined and institutionalized. Just as the construction and proliferation of locks and keys represent protection of ownership, these are also a recognition of its opposite, the possibility of appropriation of these values by others, such as theft (most common). Thus, whatever object or phenomenon a society considers valuable, appropriable and mobile, are usually stored in areas protected from free access by “outsiders”. Providing a lock to the access of this area implies a control; the possession of a key implies authorization of access. However, not only physical objects are guarded by means of locks; information that needs to be kept private (secret) are also locked or made inaccessible by a variety of methods. One of these is by means of mystifying the message by using cryptography, which makes the information incomprehensible to outsiders, those who do not know how to decode, or unlock its meaning.

The basic, functional principle of a lock mechanism is the fusion of two disparate, yet complementary parts, the key and the lock, with a perfect (mechanical) match, this match enabling the movement (usually by rotation) that causes the release of a bolt or a bar, for the purpose of:

- *entry*, such as the opening of a door, lid, etc., or,
- *release*, as with padlocks and similar locks used for locking bicycles, handcuffs, etc., for keeping an object (or person) from moving away.

The fusion of the two complementary parts is made by the insertion of an outside object, the key, into an opening in the lock mechanism, such as a keyhole. This configuration of parts may stir the imagination and symbolic thinking ability of some, even enticing this because of the insertion and the twisting motion required for a successful release of the lock, as evident in engineering terminology that sometimes call two, complementary parts such as a key and a lock for 'male' and 'female' respectively. Whatever way the act of locking or unlocking and the complementary parts are called or interpreted, the basic, trivial function of unlocking is to

open up something which otherwise is closed, inaccessible or immobile; the opening and closing being designs created for the intension of control. As Bruno Latour points out (Latour 1992) the use of doors, keys, locks and door pumps are *convenient delegations* from human beings, of numerous social and physical functions, to a variety of technological objects intended to serve these purposes. As evident in any parking lot where car owners snugly press the remote control lock mechanism of the car (infrared waves that operate relays, which in turn control the locks, usually by means of a magnetic mechanism, which responds with a two-toned beep), this delegation may involve numerous technological solutions based on a few objectives:

- *control of access* into an enclosed domain at a point of entry, such as a door, or a gate, lid, drawer, cupboard, refrigerator, etc., obstacles or wickets that keep small children away from staircases, electric sockets, etc, or a 'virtual' space, as entry into a computer-based system. In some cases, this also involves the *control of exit*, such as in a prison or animal pen,
- *control of a material object*, which due to its size or other characteristics are mobile (wheels, automotive capability, etc), such as money, documents and other valuables of small size, or larger mobile objects, such as cars, boats, bicycles, etc.,
- *control of humans or animals*, such as with handcuffs, chains, etc.,
- *control of information and communication*, so that content is kept private, i.e. remains secret to the outside world.

As evident in the history of technology, numerous solutions to these objectives have been designed. Thus, the emergence, diffusion and evolution of various types of keys and locks mirror socio-cultural and political conditions of the society in which they have existed. One interpretation provided by a historian of lock technology (Wiig, p.12) claims that the development of lock technology correlates with the political and moral situation in a society, as evident in ancient Rome, in which the technology of locks evolved in terms of sophistication and ingenuity as the moral standards of Rome deteriorated. Similarly, in more recent history, the advent of modern, more 'unpickable' locks (Chubb, Yale, etc.) came with the social unrest of the industrial revolution, in which crime, in particular burglary, became rampant. In this, as the industrial revolutions itself, England played an important role. During the past thirty years these objectives have also entered cyberspace, into the virtual world of information and communication systems. In this, smart cards have, ever since their early development stage, been appreciated for their potential of becoming 'virtual' locks and key, as will be elaborated soon.


The first locks that archaeologists have found are dated to 4000 B.C., in remnants from ancient Egypt, where these locks were made of wood, thus being fairly large and bulky by modern standards. However, the mechanisms of these early locks were in principle identical to the modern Yale-lock, the type of mechanical lock that is most common in our everyday lives. In recognition of this, this type is called an Egyptian lock. Most of us are burdened to carry around numerous keys, in order to move around in modern society. In addition, we are required to memorize a number of passwords in order to enter into

computerized information systems. As the emergence of keys and locks accompany the development of civilization as a distinct characteristic, some observers of lock technology note that even in societies that are classified as simple and egalitarian, one may find some type of technical solution for the regulation and control of the domicile. Thus entry doors are often bolted from the inside of a house, so that its inhabitants may live and rest without inconvenient surprise attacks or visits – i.e. the doors are blocked for the protection of privacy at home. In this, the 'code' of a closed entrance door is: please do not disturb. In some societies, such as at rustic inns in the countryside of France, instead of a bolt or a latch, the doors to the guestrooms were 'locked' by a thin rope which the guests fastened on a nail on the door frame, this securing the needed minimum of privacy as this would deter outsiders from bursting into the room. In some 'lockless' societies, symbolic locks are used, these signs indicating an area or space that should not be trespassed, e.g. a sign that symbolizes that a visitor should abstain from entering a house. In the remote, isolated valley of Setesdal in pre-modern Norway, posting a sweeping broom to the main door of the house served at this type of signal. Entering the house by moving away the broom (in the absence of its inhabitants) was considered breaking a tabu, thus condemned as being indecent behaviour, worse than burglary. Thus, in most societies, even in nomadic or semi-nomadic societies where people live in tents, etc., the idea that some areas are non-public and private because these belong to a sphere of intimacy, make people construct and use technical devices in order to enforce this, usually a door, at the point of entry. Of course, a door also serves as protection against cold and wild animals and a host of other functions, such as keeping children and elderly senile from straying away. Thus, the range of applications of locks and keys are numerous. In spite of this multitude, one may basically distinguish two types of locks and keys: Mechanical/physical locks and information-based locks. In addition to these, there are numerous hybrid or mixed, intermediary varieties that combine some elements of both types. Below, these will be elaborated.

Mechanical locks

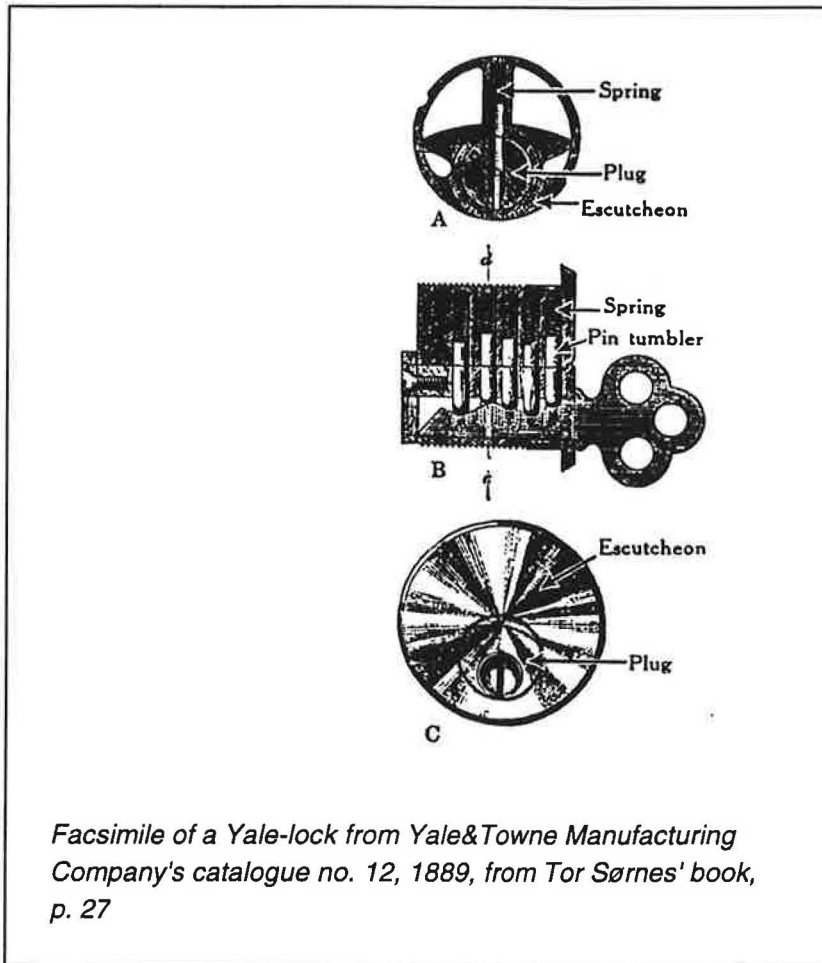
Most of us are intimately familiar with locks and keys because these are integral parts of our modern, daily life. A normal adult usually carries a number of keys close to his or her body, in pockets or handbags, in order to gain convenient access to flats, rooms, houses, cars, filing cabinets, etc.³⁹. A typical, modern 'accident' is to forget ones keys at home in the morning, as the door of the house is automatically latched upon the hurried and absentminded rush to work. The implications of this is that the business of doing business as usual become difficult, if not impossible⁴⁰.

Mechanical locks – and the keys that work with these – may be classified according to their design. As evident in exhibitions in technical museums, the variety of lock designs is large, however, three basic types predominate:

- *Yale-locks*, which function according to a technical principle similar to the original, ancient Egyptian locks from 4000 B.C., have a high degree of dissemination. When inserted in the right lock, the jagged teeth of a Yale-key () will lift a series of pins upward to a position that enables the rotation of a cylinder. This, in turn, moves the bolt of the lock. Yale-locks carry the name of its inventor, the American Linus Yale sr., who in 1844 designed a lock based on precedents found in the Bramah-lock, see below, however by making his own unique design.

³⁹ In writing this, I made a quick survey of the keys I carry with me during a normal day. In total, there were eleven keys. These were: 2 keys for my home, 3 keys for one of the offices I work at, 2 for the other office, 1 for my car, 1 for my bicycle, 2 for the filing cabinets at my office. All the keys were of the Yale-type. In addition to these, at home and in the office, I have many keys that will give me access to other spaces, but these I use less frequently, so they are not carried around all the time. One of these is the key to my boat, which is stored in my summerhouse, together with the key to gate to the harbour where the boat is moored and the key to the boat house in the harbour, where the gasoline tank is stored. The key to the summerhouse I keep in my car, etc. Of course, this is highly anecdotal evidence, however, not atypical, because many people may give similar accounts.

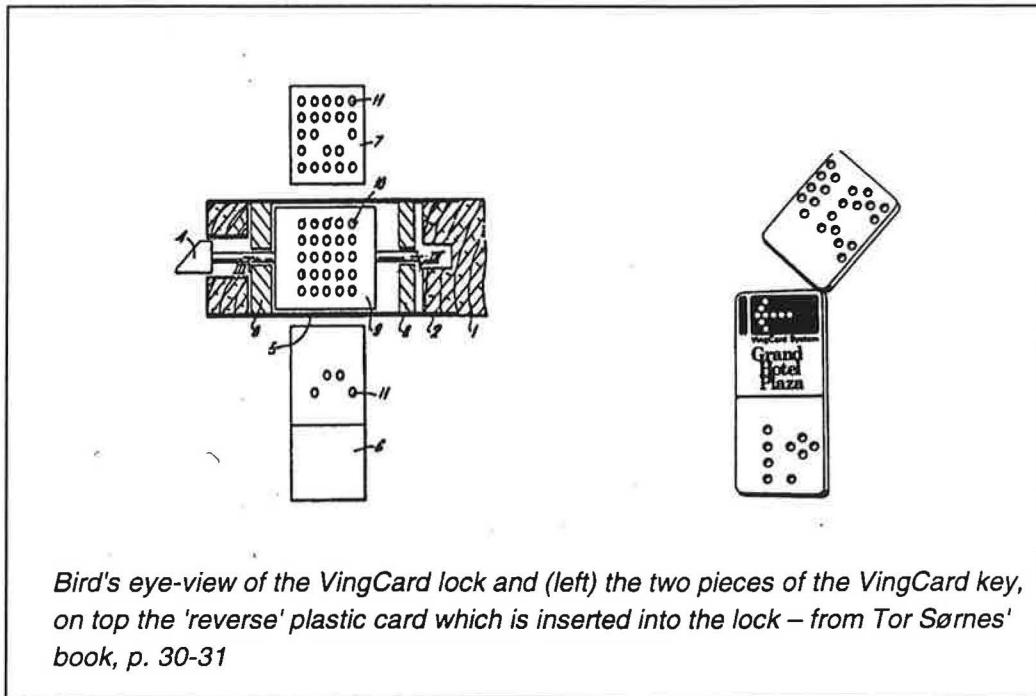
⁴⁰ One not unusual chain of events that this type of calamity causes is to first borrow a telephone from a kind person in order to call a locksmith, who, if he is compliant and competent, will pick the lock to the apartment for an outrageous prize. Thus, with a two or three hours delay, and to a considerable private and totally unanticipated expense, one may resume business as usual.



- *Warded locks*, which were originally designed in ancient Rome, is based on wards variously shaped inside the lock. Unless the key's shape is a negative of the wards, these will block access to the bolt-moving cylinder. Warded locks had a high rate of use prior to Yale-locks – a warded lock key has the classic key (⚔) profile and shape.
- *Bramah-locks*, which were patented first in 1784 by the English inventor Joseph Bramah, use tubular keys with slots in its ends. When the key is inserted in the keyhole, the slots press a number of movable slides of different length in the lock. At the 'right' distance, the key may be rotated, thus engaging the cylinder, which in turn throws the bolt. This type of lock has many similarities to the design of ancient Chinese and old Nordic locks and padlocks, as these also used pin-shaped, slim keys.

As the design of keys and locks has evolved, numerous hybrid versions of mechanical locks have been designed. As pointed out above, some design features in the Yale-lock have antecedents in Bramah-locks. Conversely, in the design of some 'high-security' locks, which may look similar to the pencil-shaped keys of Bramah-locks, the key has longitudinal taps and tracks on the side of the rod, as in Yale-keys. In some locks, magnets and electric relays are used in conjunction with keys in which miniscule magnets are inserted, so that when the key is in the right position, the movable parts will respond, such as used in many cars having a

central lock system. However, the basic mechanisms of these locks are usually fairly similar to purely mechanical locks.



Perhaps one of the most ingenious modern mechanical locks is the VingCard lock designed by the Norwegian engineer Tor Sørnes and initially patented in 1977 (US Patent 4,149,394 – filed in 1979). The technical principle is also almost identical to the ancient Egyptian lock, however, in the reverse, as a negative. Thus, instead of a key that looks like a toothbrush, which was the profile of an Egyptian key, the VingCard key is a flat plastic card with a variable number of holes (approx. 3 millimetres in diameter), these organized according the coordinates of a matrix. This matrix is complementary to a matrix of taps inside the lock; in some locks the matrix has 5 * 5 taps, in others 8 * 8 taps, i.e. in the latter 64 taps in total for which approximately 2 million different positions, or unique keys are (theoretically) possible. In constructing a key by drilling or punching holes in the plastic card, a "negative" matrix is simultaneously made on an identical piece of plastic, which is inserted permanently in the lock, blocking the taps in the positions that have no holes. Thus the taps that pass through the drilled holes in the plastic card (the "negative" card) inside the lock activates the locking mechanism. When the "positive" plastic card is inserted, these lift the taps, thus releasing the locking mechanism, this enabling opening a door. The VingCard lock has had success in hotels and office buildings because if keys are lost (which happens often), redesigning a key is simple, this being inexpensive compared to conventional keys, simultaneously reducing the fear that lost keys may be found and used for unauthorized purposes.

In general, due to modern precision tools and automated manufacturing equipment, the quality (strength and "unpickability") of locks has increased greatly as the price has decreased. Still, the basic mechanical principles of modern locks and keys were designed thousands of years ago, in the early civilizations. Thus the antecedents of modern mechanical keys have in fact existed for a long time – the basic designs used today represent thousands of years of gradual, evolutionary development.

Information-based locks

These consist of basically two types: Passwords and cryptography. As with mechanical locks, elements of both types may often be combined. In addition, information is used in combination with mechanical varieties, such as combination locks, in number codes (e.g.: first turn to 5, then to 35 by clockwise rotation, the back to 13 in a counter-clockwise rotation), i.e. many hybrid varieties exist. As with mechanical locks, the antecedents of cryptography and passwords may be found in the history of ancient civilizations, thus the history of information-based locks in many ways mirror that of mechanical locks and keys. However, the early history of passwords is not so well documented as with cryptography, perhaps because of its simplicity in use and management. Outside the world of ICT, passwords are often used as a means to gain access to places that are guarded. In banking, a password whispered into the ears of a bank officer is used as a supplementary guard for the access to a bank's safety deposit vaults. At military camps, a password of "today" is given to soldiers who go outside for short leaves, so that when they return, they may freely pass the guard if the right password is uttered. A hybrid variety of a password is the use of a coin or a money bill which has been divided or broken/torn unevenly, so that when two contracting parties want to make certain the identity of its counterpart, this is authenticated if the two parts of the coin or bill match perfectly at the perforation. The mass proliferation of passwords, especially of PIN-codes, is a fairly recent phenomenon related to access to computers and ICT-systems. Being secret, providing the right password or PIN-code serves as authentication of the user's identity and authorization of a transaction. As the user enters a password or a PIN-code in the ICT-system, this is compared with the password or PIN-code stored in the system. For this reason, password-files are considered strategic and vulnerable, these being guarded as the ultimate secret. Thus, being able to penetrate into a password file is considered a major feat among hackers.

An emerging field of password is the use of biometrics as identification of a user. A biometric password (possibly a misnomer) is based on the principle that a unique individual characteristic of a person's body, such as the voice, finger-print, the iris of the eye, or even the face itself, may be recognized by a computer-system, and by this, the computer will verify the identity of the person to whom these bodily characteristics belong. At present, numerous biometric systems compete to enter the "ICT-security" market, however, fingerprint pattern analysis are apparently leading this race. The French smart card manufacturing firm Schlumberger recently (May 2001) signed a contract with the US Department of Defence, for

the delivery of 600.000 smart card based ID-cards, to be used by military employees.⁴¹ In this, finger-print analysis capability is provided. These ID-cards will also have a picture and the signature of the person, and store other types of information about the person's physical attributes (gender, age, height, colour of skin, eyes, hair, etc.). In a press release in February 2002, Schlumberger announced that it had successfully developed a voice recognition (authentication) system to be implemented in the SIM-card (i.e. smart card) of a mobile telephone handset produced by Mitsubishi. The technological advantage (Schlumberger called this "a security breakthrough") of this is that it does not require any additional equipment in the mobile telephone; only the software (voice authentication algorithm) for analysing the voice pattern, this software would reside in the SIM-card, thus being tamper-resistant⁴². Finger print pattern analysis, in contrast, requires a specialized scanner for recording the image of a fingerprint, i.e. a separate equipment unit. Numerous equipment manufacturers are offering finger print scanners for biometric key applications; however, the response from the market has so far been hesitant. One type of finger print analysis equipment called *Big Mouse Plus*, produced by the US smart card manufacturing company ActivCard, is a combined smart card reader and a finger print scanner, which may be connected to a PC by means of the USB-port⁴³. The finger print scanners usually have the size of a large matchbox, with an oval lens (approximately 4 cm in diameter). As a user puts one of his or her fingertips on this lens, the scanner will transmit the recorded image to a file and compare this pattern with the ones that are stored in the memory of the smart card (or PC) as authorized. If these match, then the user may proceed to other applications. One Norwegian upstart company, Idex, has developed a biometric finger print scanner integrated with a numerical keyboard that controls the lock of a door. One idea for applying this is for doors to safe strong boxes and high security buildings and rooms. This, as most other biometric systems, requires the user to enter a PIN-code in addition to the fingerprint. Thus, the manufacturers claim that a combination of two password systems (PIN-code + biometric pattern analysis) will provide a very high degree of security.

⁴¹ Cf.: http://www1.slb.com/smartcards/news/01/sct_dod1405.html - the price per smart card in this contract was US\$ 7,50. According to a spokesperson from the US Department of Defence (DoD) who held a briefing about this contract at the "Cartes 2001"-exhibition in Paris in October 2001, the DoD was planning to expand the use of this smart card ID-system, to the entire DoD, and to add numerous applications to the card, such as digital signature (asymmetric crypto-key), security authorization, etc.

⁴² Cf.: http://www1.slb.com/smartcards/news/02/sct_voice1902.html

⁴³ Cf.: <http://www.ankari.com/biomouse-plus.asp>



ActivCard's Big Mouse Plus, with a finger-print scanner (the oval lens on the top, right) and a smart card reader, also on the top, left.

In the universe of passwords, the main purpose of these is, by means of information, to control the access or entry into an enclosed area, whether these are real, tangible and physical spaces, or the virtual spaces in the ICT-world. In the terminology of ICT, this is called authentication, the process of proving the real identity of someone. An additional function, such as with PIN-codes, is to provide authorization, the ICT-version of saying "yes", i.e. the expressed agreement or approval to something, such as entering the PIN-code when paying for merchandise or services with a plastic card.

Cryptography

The craft and art (it is increasingly becoming a science) of cryptography is also old; just as the technology of locks and keys may be traced to ancient Egypt, so historians of cryptography claim that a cryptographic variety of hieroglyphics was developed and put into use by the Egyptians – and also in ancient Mesopotamia, as archaeological evidence indicate cuneiform characters written on clay tablets in a manner that has been interpreted as the use of code in order to hide a message. The main purpose of cryptography is to hide the true, or *plaintext*⁴⁴ meaning of a message by means of a code that only the sender and receiver will understand, so that if the message is intercepted, the content of the message does not make any sense to the interceptors. However, for technical reasons, the methods of cryptography are used in modern telecommunications, called signal coding, especially in digital communication. In this, the codes are not secret, as evident in the ASCII-standard that assign a digital code (series of 1 and 0) to the characters of the alphabet. Digital signal coding provides numerous

⁴⁴ 'Plaintext' is the term used in cryptography for a text or a message before it is coded – i.e. the intended content of a message.

advantages in terms of quality, because this makes it possible to recreate an identical message to the one that was transmitted as the problem of noise is avoided. However, "real" cryptography is a method for controlling the content of a message so that the recipient may only understand it. There are many ways of doing this. One variety called *steganography*⁴⁵, is to hide the message completely, in addition to encrypting it. In the murky history of cryptography, the techniques used for hiding the encrypted message have a central role, such as the writing of an encrypted message with invisible ink, in-between the lines of a "legitimate", innocuous letter. During WWII, the German intelligence community became known to use microdots (miniaturizing the size of the writing by photographing the text using a "reversed" microscope so much that it appears as a dot, i.e. the size of a period or a quote-mark, etc) seems to have been a popular technique. Some spymasters are worried with satellite television using digital signal codes and the Internet because they think that encoded messages may be hidden within complex graphical codes, i.e. in the dense jungle of bits. The technique of mingling a message with the crowd evolved parallel to the emergence of mass media, in particular the use of classified advertisement in newspapers, some claim, may often contain encrypted messages, e.g. a used cars classified ad such as "Toyota Hiace wagon, red, 1989-model, 225.000 km, no rust, motor recently overhauled, price: [a number stated], tel: [a number stated]" may really be a message giving instructions or information to a spy, a corrupt bureaucrat – or a secret lover.

Just as the technology of locks and keys imply recognition of the inevitability of burglary and other varieties of expropriation, cryptography implies a recognition that information and communication may cause some kind of impact to the parties involved, if this is not kept secret, this irrespective of the motives or objectives for using cryptographic "protection". In the extreme type of cryptography, such as stagenographical messages that try to hide the very act of communication, the sender and receiver also wish to make the relationship invisible, completely secret. Still, in spite of the covert, conspiratorial nature of cryptography, its design and intention, there seems to be a very basic social and cultural foundation for its use, as evident in the ideals of privacy (which most cherish) and otherwise in normal social intercourse. Thus, one may claim that the phenomenon of gossip and spreading of rumours in everyday social life involve the management of information in various codes (e.g. all the subtleties of body language), withholding information to some, providing twisted interpretations to others, hints, planting, etc. in an elaborate social choreography, which has many parallels to the use of cryptography. In this the use of coded information and signs, such as a "secret", almost invisible wink with the eye to someone at a strategic moment, may indicate that the use of coded communication is socially universal, as informal, "soft" cryptographic systems are integral parts of normal social interaction.

In modern time, as the art and craft of cryptography has evolved, this has gradually developed into an advanced mathematical discipline. As pointed out earlier, the distinction

⁴⁵ Because the art and craft of cryptography often is employed for the purpose of deceit, at times it may be opportunistic (e.g. to create confusion or mislead someone) to let an encrypted message be intercepted, even to use a code that may easily be cracked in cryptoanalysis.

between different types of applications have gradually become blurred as cryptographic methods are essential to signal coding in many types of telecommunications, in particular in digital communication. The distinction is now more in terms of degrees, i.e. the degree of openness or secrecy related to coding techniques and methods. However, as with the technology of locks and keys, the basic principles are few and simple:

- *Transposition*, in which the elements that constitute a message are rearranged, without changing the elements themselves, such as when "hello" is encrypted as "olleh" (spelling backwards, very simple code, however, it is claimed that Leonardo da Vinci used reversed writing method in his sketch-book, making the text illegible without the use of a mirror).
- *Substitution*, in which the text is replaced by another element, i.e. transcribed to a new order, such as encrypting a telephone number by adding 1 to each number, i.e. making the plaintext number 22 59 51 00 become 33 60 62 11 (also very simple, however this cryptation method was used in 1973 by Mossad agents during their assassination of Ahmed Bouchiki in Lillehammer in Norway, in order to "hide" the telephone numbers of their contacts in Norway).
- *Combinations of transposition and substitution*, by various hybrids, permutations and elaborations of the two. One standard cryptation system widely used and known as DES (Data Encryption Standard) encrypts a message by 16 rounds of transposition and substitution, a process which should make any message impossible to decode, if not in theory, then for all practical purposes.

Once a message has been encoded and successfully transmitted, the process of decoding starts, in which the metaphor of lock and key is used, i.e. "unlocking" the content of a message, by inserting and "twisting" a key around. There are basically two types of keys: *Symmetrical* and *asymmetrical*. In the former, the sender and receiver use identical keys, i.e. the receiver decodes the message by reversing the encoding procedure using an identical key (code), thus this is also called a *single-key* system. The DES crypto-system mentioned earlier is based on symmetric keys. In the asymmetrical key system, which has become widespread because of Internet's success, and is also known by its acronym PKI (Public Key Infrastructure), a *two-key* system is used: One set of keys that is public and a single key that is private (secret). Being technically and computationally complex, the basic mechanism is simple: The receiver (B) of a message has a number of keys which may be used for encrypting a message, i.e. public keys, however, only one that may decrypt all these, i.e. the private (secret) key. The sender (A) chooses one of the public keys (e.g. downloads it from B via the Internet), encrypts the message and sends it back to B. B then uses his private key to open the message. Because only B has the key that will decrypt the message, B may be fairly certain that the message has not been tampered with, and, if intercepted, that the interceptor will have great difficulties in undertaking a cryptanalysis, i.e. try to decode the message. The most widely used asymmetric key system is known by its acronym RSA⁴⁶. Asymmetric keys

⁴⁶ RSA is an acronym based on the names of Ron Rivest, Adi Shamir and Len Adleman, the men who originally invented the algorithm for this key in 1978, at that time professors in computer science at MIT.

are used as *digital signature* which during the past years have become legally equivalent to ordinary signatures.

According to experts, there are advantages and disadvantages in relation to both symmetric and asymmetric keys. The weakness of symmetric key system is related to the management of keys, because ideally, in order to attain a high degree of security, each bilateral relationship in a network will need a unique key. For this reason, the number of required keys will increase exponentially as the size of a network grows. Thus, the cost of a symmetric key system will also grow exponentially, which is a drawback in itself, however, the administrative tasks of keeping track of all the keys is also difficult. In connection with this, the problem of trust and authorization of keys becomes delicate as the sized of a network grows, which in itself is considered a security risk. These problems are much smaller in an asymmetric key system because each user has his or her own private key, thus the number of keys will increase only proportionally to the number of users in a system. The disadvantage of an asymmetric key system is that these are very demanding in terms of processing requirements, the implication of this being that they are much slower than symmetric keys. The RSA asymmetric key uses an algorithm derived from the multiplication of two very large prime numbers, which in turn create keys that are complex. In spite of the computational powers of modern computers, this key inevitably demands relatively long execution time. Thus, asymmetric keys are (with present computing speeds) not well adapted for applications that are information heavy, such as multimedia and video signals. As symmetric keys are much faster, these are better suited for these types of applications which need to decode or encode much information at high speeds and in which the requirements for secrecy may not be imperative.

Lock-picking and cryptoanalysis

These two activities, or methods, are similar in terms of purpose and mode of work, because both use stealth for overcoming the obstructions set by mechanical and information based locks, in order to gain access to, or possession of, whatever is made inaccessible by these types of locks. Using tools that simulate the original keys, this is done by manipulating the locking mechanism. Thus both methods require a good understanding of how the locking mechanism works. In the case of mechanical locks, the lock-picker must understand the lock's design and construction, how moving parts act, etc. Usually, a lock-picker uses a tool called rake pick, but according to insiders even a safety pin or a slim screwdriver may serve as tool. These tools are inserted into the keyhole and diligently manipulated until the lock opens. In the cryptoanalysis, which is the technical term for the decoding undertaken in picking information-based locks, knowledge of cryptography and related disciplines of mathematics and information and communication theory is advantageous. Furthermore, as both methods are based on tools that simulate the actions of the real keys, picking locks and doing cryptoanalysis is often undertaken in order to disguise the act of penetration. Whereas the common burglar simply uses a crowbar or a wrench to break up a door (causing much noise

and damage) the art of picking a lock requires skill, patience and time. Similarly, undertaking cryptoanalysis requires skill and patience. The stealth and skilfulness involved in disguising the act of penetration may be motivated by a number of different considerations, however, the deceit or trickery involved is a salient characteristic. To the victim this conveys that someone in his or her environment does not need to use brutal force to gain access to whatever is locked – this 'someone' possesses tools and skills that in effect give them full access. Understandably, people who suspect or are certain that their locks have been compromised by 'false' keys become anxious.

In the history of locks and keys, there is a parallel history of lock-picking and cryptoanalysis. However, whereas the history of cryptography, in spite of the secrecy that veils these types of activities, has been chronicled in numerous books and documents, especially in biographies that commemorate the secret, heroic work of some cryptanalyst, the history of lock-picking is not so well documented. The latter may be due to its artisan nature, however, if the word 'lock picking' is written into a search-engine in the Internet, the response is overwhelming⁴⁷. Perhaps the main reason why the history of cryptoanalysis is comparatively well documented is that most governments, for the sake of 'national security', have established specialized agencies entirely devoted to cryptoanalysis. These agencies have employed academics, often mathematicians, who sooner or later write their memoirs or make contributions in professional and academic contexts⁴⁸. During wartime, especially during WWII, the use of cryptoanalysis for military intelligence greatly boosted the size of the cryptanalyst communities in almost all the parties involved. By far the largest cryptanalytical organization at present is NSA – National Security Agency – of the US government⁴⁹, possibly larger than the CIA in terms of number of employees and resources. NSA literally eavesdrops on the entire earth in its electronic surveillance activities. According to insiders, NSA has one of the largest and most powerful computing facilities in the world (Kahn 1996; Levy 2001). In addition to mathematicians, NSA claims that it is 'one of the most important centers of foreign language analysis and research within the [US] Government'⁵⁰. Thus, the most powerful nation of the world in military strength also has the largest cryptanalytical organization. This illustrates that cryptoanalysis is considered strategic for the maintenance of world political and military hegemony. The rhetoric of governmental

⁴⁷ On 7 March 2002, as a test, I typed "lock-picking" into the Google search machine. This yielded 14500 "hits". Judging from the first pages of the responses, most of these were links to companies that offer lock-picking tools and instructions.

⁴⁸ Charles Babbage, who many claim was the real inventor of the computer, has written 'Picking locks and deciphering', chapter 18 in his autobiography from 1864, *Passages from the Life of a Philosopher*, which may also be found on the web at: <http://www.fourmilab.ch/lockpick.html>

⁴⁹ Cf.: <http://www.nsa.gov> - NSA's homepage – displays the organization's motto: 'Providing and protecting vital information through cryptology'. NSA claims to be the 'largest employer of mathematicians in the United States and perhaps the world'. NSA's homepage has a link to its museum, a section which contains numerous interesting historical articles, such as NSA's activities during the Korean war in the early 1950s.

⁵⁰ Cf.: http://www.nsa.gov/about_nsa/index.html

organizations specializing in cryptanalysis is that this provides 'intelligence' vital for the national security by surveillance of activities that may be subversive, typically justified by paroles such as 'we protect democracy and freedom'. Thus, the ambivalence of using methods of disguise (unlocking other's secrets by means of cryptography), which are inherently illegitimate, is justified in terms of noble causes.

Be this as it may, the government employed cryptoanalytic communities have expressed concern about the sophistication of various signal codes and commercial, civilian cryptographic methods that have been developed because these may make their cryptoanalytical tasks more difficult. Thus, the signal code used in GSM has been a source of conflict between telecommunication operators and various governmental agencies that have a legitimate right to eavesdrop on the conversations of mobile telephone users. Similarly, the RSA was for a long time classified as 'strategic technology', for this reason it was on an US export limitations list (Kahn 1996; Levy 2001). During the 1990s, the large-scale diffusion of Internet and its claimed notorious lack of security have increased the demand for commercial, civilian cryptographic systems.⁵¹

Lock picking and its history may be analyzed in a perspective of reverse engineering, or reverse technology design. As evident in computer hacking, the capability to penetrate into an area "protected" by a lock may be acquired by a trail and failure approach, often based on guess-work, which in turn contributes to a learning process which will make the lock-picker (or hacker) skilful in terms of penetration. Simultaneously, one may assume that the lock-picker in this process acquires a functional understanding of the technology, which may be basic. According to Bruno Latour, in his essay on the "Berlin lock" ((Latour 1992)), the notion of *anti-program* describes the technological modifications undertaken on the key in order to make it more convenient for its lazy and nonchalant users. In Latour's explanation, technological devices and designs may be considered a *delegation* of functions from humans; with locks this is the delegation of control functions undertaken by the watchman or janitor to a special type of lock, the Berlin lock. Thus in the lock, the delegation is embedded as a *program* in the technical design. The uniqueness of the Berlin key's design, or program, is that it forces the users to relock the gate-door – the key is not released until the door is locked. According to Latour, some of the users of this lock, who are lazy and do not want to be bothered by the pedantry of relocking the gate-door each time they pass, have modified the key so that it may be released without relocking. This modification, Latour calls an *anti-program*. The explanatory attractiveness of using the dichotomy of 'program' and 'anti-program' is that it relates the design, construction and use of locks to the actions related to the technology: The focus is set on why people design and install locks (the program) and, as a contrast, why other people modify this design in order to make the very same locks impotent,

⁵¹ The right to keep communication on the Internet secret has been one of the basic civil rights promoted by the EFF – the Electronic Freedom Foundation – cf. <http://www.eff.org/privacy/> - as the fundamental right to send messages encrypted. This encompasses an opposition to the idea promoted by some governmental cryptoanalysts, that the institution of 'trusted third party' should be administered by them, giving them access to the secret private keys used in encrypting communication, order to simplify their surveillance.

or pervert/dilute their intended functions, as anti-program. In Latour's conceptual framework, the introduction and installation of a lock in an area or on an object is the technological (or 'convenient') implementation of a regulation of social relationship, which is more precise than a program. Following the logic of Latour's explanatory strategy, it may be more fertile to mobilize the term *regulation*, and its antonym *deregulation* and its modification as *reregulation*, in order to depict the powerful dialectics involved in the design and construction of technology. The advantage of using the term 'regulation', instead of 'program' for the analysis and explanation of locks and keys is that this relates more closely to the teleological aspects of technology, in particular the socio-political and economic reasons why people and social systems use locks – and why others oppose this by using a variety of methods for this purpose, i.e. their strategy of deregulation. This may be demonstrated by a case of deregulation strategy that has, according to one reliable source, been demonstrated for biometric keys. Biometric keys, as a smart card application, are by proponents claimed to be almost impossible to “compromise” – in particular biometric keys based on fingerprints are regarded as “foolproof”. Thus, biometric deregulation, apart from amputation of someone’s finger, has been promoted as impossible. In addition, by using biometric keys, the mnemonic problems associated with PIN-codes are eliminated. This may explain why numerous organizations have made statements that they intend to adopt smart card solutions with biometric keys, in particular fingerprint biometrics, in order to “increase security”.⁵² However, the deregulation strategy of fingerprint biometrics is claimed to be very simple:

“Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices./.../ Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and \$10 worth of household supplies.

Matsumoto uses gelatin, the stuff that Gummi Bears are made out of. First he takes a live finger and makes a plastic mold. (He uses a free-molding plastic used to make plastic molds, and is sold at hobby shops.) Then he pours liquid gelatin into the mold and lets it harden. (The gelatin comes in solid sheets, and is used to make jellied meats, soups, and candies, and is sold in grocery stores.) This gelatin fake finger fools fingerprint detectors about 80% of the time.

His more interesting experiment involves latent fingerprints. He takes a fingerprint left on a piece of glass, enhances it with a cyanoacrylate adhesive, and then photographs it with a digital camera. Using PhotoShop, he improves the contrast and prints the fingerprint onto a transparency sheet. Then, he takes a photo-sensitive printed-circuit board (PCB) and uses the fingerprint transparency to etch the fingerprint into the copper, making it three-dimensional. (You can find photo-sensitive PCBs, along with instructions for use, in most electronics hobby shops.) Finally, he makes a gelatin finger using the print on the PCB. This also fools fingerprint detectors about 80% of the time.

⁵² Cf.: <http://nettavisen.no/servlets/page?section=59&item212711> - a Norwegian Internet news service, 6 May 2002 edition, article “SAS vil ha fingeravtrykket ditt” [“SAS (Scandinavian Airlines System) wants your fingerprint”]. According to this, SAS was considering introduction of fingerprint biometrics of its passengers, as a measure to increase security during flight check-ins and embarkation.

Gummy fingers can even fool sensors being watched by guards. Simply form the clear gelatin finger over your own. This lets you hide it as you press your own finger onto the sensor. After it lets you in, eat the evidence.”⁵³

Discussion – continuity and discontinuity?

The ancestry and technological origin of locks and keys may traced back to the early civilizations of Egypt, Mesopotamia and China, i.e. archaeological evidence dates this to thousands of years B.C. As evident in the technological principles that operate the family of Egyptian locks, there is a strong continuity in terms of design from these early locks and keys – to contemporary versions, such as locks and keys of the Yale type. Most modern, urban people carry a bundle of keys, usually Yale-keys, with them as a standard outfit, just as natural and basic as wearing shoes. However, the use of regulation technologies is not just a civilization technology. Even in nomadic or peasant societies, societies that are considered “lockless”, people use technological solutions (however rudimentary) in order to provide protection to themselves, i.e. uphold some kind of shield between what they consider intimate or dear – and the outside, public world or wilderness. This is done by various means of bolts, ropes or more symbolic devices that keep doors closed or areas enclosed. Thus regulation of space and values seem to be universal – most societies employ technological solutions in order to achieve this. This supports Basalla’s gradualist claim that continuity rules in the development of technology. Furthermore, that analysis of technological development must distinguish the social impacts from technological evolution, because the technological evolution of locks and keys, such as the Egyptian type, cannot explain social development.

However, on closer inspection, Basalla’s claim is not so obvious. Explaining modern society and its regulation technology as having evolved gradually, being based on predecessors and antecedents does not provide satisfactory technological explanations to inherent technical characteristics and to the variety and diversity of locks and keys being used today. Most obviously, the smart card, with its embedded microprocessor and its capability of processing electronic information and software, did not exist prior to its invention late in the 1960s and early 1970s. The ideas of this type of solution existed as a fantasy in the science fiction literature, however, nowhere else prior to its invention. Whereas a mechanical lock and key is mono-functional because its construction is designed for a single purpose (e.g.: to regulate the opening and locking of a door), a smart card is multifunctional and versatile; whereas the former is “dumb”, the latter is “smart”. Thus, following Basalla’s hypothesis would not provide a satisfactory technological explanation to the emergence of modern, ICT-based locks and keys: In fact, these represent technological discontinuity in a number of ways.

Furthermore, Basalla claims that analysts who adhere to the possibility of technological discontinuities (e.g.: “radical innovations”) confuse social impacts with

⁵³ Cf. Crypto-Gram Newsletter, article “Fun with Fingerprint Readers”, by Bruce Schneier, 15 May 2002, downloaded from: <http://www.counterpane.com/crypto-gram-0205.html>

technological novelties: The “industrial revolution” was a radical social shift, i.e. a period of rapid social development and change, not technological, because the technological innovations (e.g.: steam engines) had emerged gradually during a period of two centuries, as the result of a slow evolutionary process. The basic structure of this claim does not fit into our contemporary society: Quite on the contrary, one could claim that in analysing the power relationships and distribution of wealth and valuables in modern society, the preservation of existing social order may be the main incentive for the quest for radical technological solutions, a “burning desire” for radically improved regulation technologies. However, the matter is more complex because of ICT and cyberspace (technological discontinuity) – and its interaction with the physical, material world – a world full of tangibles and symbols, which are rapidly co-evolving with cyberspace into something novel. Contradictions and paradoxes rule in this, making Basalla’s distinction even more irrelevant. In order to explore this, in chapter 6, the focus will be set on the phenomenon of money. The reasons for choosing money as an object of analysis is multi-strategic, however, most important: An analysis of money may provide insights into the transformations of medium of both regulation technology (locks and keys) and values (money) – which have evolved into an electronic world, into cyberspace. In this smart card technology may or may not become an important technology – alone or together with a number of other applications that may be hosted in smart cards. For this reason, it may be fertile to understand the diffusion of smart card technology, which has been uneven, some claim erratic, as will be done in the next chapter. In order to elucidate this question, the chapter will also present the results of in-depth interviews with seventeen smart card development project leaders in Norway, thus giving insights into how the most knowledgeable persons in the smart card community think about the technology they are working with and trying to promote.

5 Diffusion of smart card technology

The evolution of smart card technology may be analyzed as a technology diffusion process. The classical, almost paradigmatic approach to explaining technology diffusion processes has been elaborated by Everett M. Rogers, in his seminal book, *Diffusion of innovations*. This book was first published in 1962, but has been revised and republished several times afterwards; the 4th edition came in 1995 (Rogers 1995). According to this, a successful innovation diffusion process may be statistically depicted by an S-shaped curve. The speed and outreach of the diffusion process is influenced by the following factors (Rogers 1995, p.15-16):

- *relative advantage* of the novelty to the user (including economic factors such as costs),
- *compatibility* of the novelty to existing solutions, i.e. its degree of interoperability to other, existing technologies,
- *degree of complexity* inherent in the novelty, such as how much training and skill adaptation the novelty requires in order to function according to its potential, which also encompasses how the user interface is designed,
- *trialability*, the degree to which a novelty may be experimented with, e.g. hands-on experience is important,
- *visibility* of the novelty – i.e. the immediate, obvious and intuitive appeal, such as evident in the success of "post-it" note pads.

However important for smart card diffusion, these factors are of a second order of importance, because in the diffusion of smart card technology, a number of system-related decisions are taken first. In most applications of smart card technology, the smart card is only one element in a large system; the decision to adopt and introduce smart card technology is taken by the system "owners", not by the ordinary users. Rogers (Rogers 1995, p. 372) distinguish at least three different types of diffusion processes, depending on how decisions are taken in terms of adoption:

- *Optional innovation-decisions*, which usually involves decisions taken by individual or small social units (e.g. families), typically in innovation diffusion processes involving autonomous objects or novelties that are independent of others, such as the decision to start using a PC instead of a typewriter, contraceptive pills, contact lenses, hang-gliding, etc. A large portion of diffusion studies focus on these types of decisions because they are important for understanding consumer choice.
- *Collective innovation-decisions* – decisions that will implicate all parties, typically political decisions taken to introduce or adopt a novelty subsequent to a consensus, majority vote or referendum, such as when a community decides to introduce fluoridation in the public water supply.
- *Authority innovation-decisions* – in which a person, usually as a representative of some kind of private or public authority, may decide that a community or organization should be encouraged or compelled to adopt a novelty, typically justified by reference to a new

law, a new policy or regulation, as evident when crash helmets were made compulsory for motor cyclists, as a "top-down" decision.

A salient characteristic of smart card technology is that it functions in relation to a *system*, physically as components, however, more virtually, as hosts for software and information storage that interact with systems outside the smart card. Thus, in analyzing the diffusion of smart card technology, focus should be set on the systems in which these are embedded. Although diffusion of smart card systems in many ways may be attributed to authority innovation-decisions, on closer inspection, this is difficult for a number of reasons because of the complexity and dynamics involved in this type of innovation-decision. In fact, the innovation diffusion processes involve decisions of all the three categories above – and at least one more. However, the primary decision is related to whether or not to introduce a system in which smart card technology has a role. The numbers of existing and planned systems that use smart card technology are not many – the exact number is difficult to count because this depends on the criteria used for defining a system⁵⁴. However, the smart cards that work in a single system are usually numerous, i.e. counted in thousands. Statistics give some indications of this: According to the 2001 statistics from the smart card industry⁵⁵, the global shipment of smart cards (chip cards as distinct from memory cards) was approximately 600 millions. Of these, 65% was supplied to the telecom sector and 23% to financial services, i.e. these two sectors account for 88% of the world smart card consumption. The third largest application of smart cards, pay-TV, accounted for approximately 4% - as this application is closely related to the telecommunications sector, one may claim that roughly 70% of the world consumption of smart cards is related to telecommunication services.⁵⁶ The geography of this global picture of smart card distribution is: European markets – 58%, Asian markets – 35%, only 7% to the American markets. Interpreting these figures, it is evident that smart card technology's dominant application is as SIM-card in the GSM mobile communication telephone handsets, i.e. as a component in a two-way communication system and service. This reflects the geographical distribution of the GSM-system, which has attained a dominant position in the "Old World". In addition, smart cards are also used in pay-TV, in reality a telecommunications service, in decoders and as a petty cash medium. Because of GSM's success, the high diffusion rate of smart card technology has followed this success, as a kind of piggyback effect. Alternately, one may attribute GSM's success to its use of smart card technology as one of its strategic components – i.e. that the engineers who designed the GSM-system were ingenious in incorporating smart cards in the system. In terms of smart card shipments, the category "financial services" is also substantial, in spite of its minority position compared with the SIM-cards diffusion. A large portion of these smart cards are deployed

⁵⁴ E.g.: Should the GSM mobile communication system be counted as one system, or should this be counted as one system per operating company?

⁵⁵ Cf.: <http://www.eurosmart.com/C-figures/C3-sectors.htm>

⁵⁶ The residual 7% comprise categories such as: "government/healthcare" (2,5 %), "transport" (1,2%), "IT/security" (0,7%), "loyalty" (1,9%) and "others" (0,7 %).

embedded in credit and debit cards, and also in petty cash cards in some European countries, notably in France.

The diffusion of smart card technology primarily reflects the expansion of particular systems designs in which the smart cards are one of numerous components. The systems' designers make the choice of technological solution and design, such as incorporation of smart card technology. In this, the primary function of the smart card is to serve as a key for the users' access to the systems: By inserting the SIM-card into the mobile telephone handset and pressing a PIN-code, the user "unlocks" the barriers, making access to the system possible and activating a number of other functions and applications. Thus, the choice of technology in a system, such as smart card technology, is made by the system designers; the users' range of choice is primarily in relationship to a system – not the individual components in the system: By choosing a system, a user inevitably (probably unknowingly) also chooses a myriad of technologies and the way these are designed to function, i.e. the user accepts the choices made by the designers.

Ideally, by entering into a contract relationship with the system, the user accepts the technological choice made by the designers of the system; in return, he or she gains access to the goods and services provided by the system. Usually, the user does not care much about the technological aspects (the innards of a system) – the user cares about the services provided; the system and its components is a black box. The basic principle of choice is "take-it-or-leave-it": A user or a consumer may choose to abstain from using GSM – and by this reject the use of smart card (SIM-card) technology – a "leave-it"-strategy. This, according to Rogers (Rogers 1995, p.372) is a *contingent innovation-decision*. However, this type of decision may also be the result of a number of composite, chained and interrelated processes, involving all the three categories in Rogers' classification. This, the system designer has to relate to – a landscape on the outside, in the markets, or external design parameters that are constantly evolving and often transient, i.e. at times difficult to discern and interpret. However, for the individual user, the extent to which a "leave-it"-strategy represents a realistic strategy to him or her depend on a number of factors, such as the availability and attractiveness of alternative means of communications, the network externalities involved, cost-benefit considerations, cultural norms, etc. On the other side of the fence, the system designers and operators, being aware of the "leave-it"-strategy as a possibility, will consider this in conjunction with other factors, which in sum reflect their judgment of their own strength and opportunities – and, conversely, the extent to which users have a real choice. In mobile communication system, the user, if he or she wants a mobile telephone, does not really have a choice because the GSM-system has a de facto monopoly – the existing alternative means of mobile communication (walkie-talkies, CB, shouting, etc.) do not provide the same level of service as GSM. In other words, the power relationship between the system and the individual user in the case of GSM is highly asymmetric, as in many "take-it-or-leave-it"-relationships. However, the system designer and owner is not omnipotent; even if his or her relationship to users is highly asymmetric, the designer/system owner has to relate to a complex set of actors who in various ways are partners, adversaries, rivals and enemies in the development of the system, in a

fluctuating, evolving landscape of techno-economic development. These may be competitors, suppliers, manufacturers, authorities, standard setting bodies, the stock market, etc.

One dimension of this may be illustrated: According to system designers in the mobile communications community, manufacturers of mobile communications equipment, such as Nokia, have attempted elimination (so far unsuccessfully) of the SIM-card in the specifications for future mobile communications systems (3G), in various standard setting bodies. Their official justification for this is that the SIM-card is superfluous – the functionality and applications provided by the SIM-card may more effectively reside inside the equipment, as an integral part of the embedded software that enables other functions in the mobile handset. The reason why smart card technology initially was chosen as an element in the design of the GSM during the early 1980s, in the technical committees of CEPT, was due to the idea of "plastic roaming" – the designers believed that the future GSM handset would be so expensive that in order to promote the dissemination of the GSM-service, users should have the possibility of subscribing to the mobile communication service independent of the handset, e.g. two or more people could share a handset, each user inserting his or her own, individual SIM-card. Now, almost twenty years later and after GSM has proved its success, mobile handset manufacturers, in their opposition to the SIM-card, rightfully claim that due to the declining price of handsets, the idea of "plastic roaming" has not materialized. In fact, the SIM-cards are more or less permanently fixed ("glued" according to one informant) to the handset. The real reason why manufacturers want the SIM-card eliminated, according to mobile system designers in the telecommunications operating companies, is not so much technical-operational considerations as a desire by the manufacturers to get a larger share of the mobile communications service market, which is now in the hands of the operators, this because of their control of the SIM-card. By eliminating the SIM-card, the manufacturers could, to a larger extent than now, market the handset directly to users, promoting their own brand names, in "packages" in which operators and service providers either are subcontractors or completely by-passed. According to informants, these types of power-struggles were played out in various technical committees in ETSI, in particular in the 3GPP⁵⁷, which was established in 1998, aimed at defining global technical standards for future mobile communication systems. However, the equipment manufacturers were not able to convince other parties as to the superfluousness of the SIM-card in future mobile communications systems – in fact, the end result consolidated the mobile operators as to the advantages in having control of the SIM-card – and its potential in the future, in particular by enhancing the concept of the "SIM-card toolkit".

In a technology diffusion process perspective, the countless of decisions and processes involved in the evolution of smart card technology encompass choice elements from most of the three categories identified earlier. Whereas this points to a diversity and complexity in the decision-making, it also points to the fact that smart card technology should be analyzed in the context of systems, i.e. the design of systems – and why some technological elements are chosen and incorporated in the design – and why others are rejected or only reluctantly

⁵⁷ 3GPP = 3rd Generation Partnership Project, cf.: <http://www.3gpp.org/> - for more information.

accepted. Extending this, one may claim that the question of smart card technology diffusion needs to be analyzed and explained in a perspective of competing systems – and why in some type of system design, incorporation and deployment of smart card technology has been strategic – and in others, this is not so obvious. Some experts of smart card technology claim that the smart card is a "technology in search of a solution", i.e. that it is a technological "fix" for which applications are not obvious – implying that the need for this is really not very urgent. However, this is too simplistic – instead one should rather ask: Why do some system designers favor and incorporate smart card technology in their solutions – while others resist or only half-heartedly deploy this? To what extent is this due to some characteristics of the smart card technology itself? How does this reflect, in comparison with alternative solutions (e.g. magnetic stripe cards) the interests of various system designers and the interests they represent? How, in terms of decomposing the S-shaped curve of smart card technology diffusion, may one explain why smart card technology's rate of diffusion has been rapid in some areas and systems, while slow and even stagnant in others?

Empirical approach

In order to elucidate some aspects of this complex set of questions, a series of in-depth interviews with seventeen informants in Norway were undertaken, in March and April 2002. The criteria for selecting informants was that they ideally should be project leaders or in a top management position in terms of a high-level, full-time responsibility of large scale smart card strategy and development project, which most of them had. Thus, their views and modes of thinking reflect the most informed minds in the Norwegian smart card development community at the time of the interviews, in a small, but wealthy and technologically advanced ICT nation. In addition, the companies and organizations they worked for had a dominant or significant position in the markets or sectors that they operated in. For this reason, although seventeen informants may be considered a small sample, these informants significantly represent the universe of smart card development and deployment in Norway because they work for systems that either encompass most of Norway's population (e.g. informants in the mobile communication companies control more than 95% of this market of 3,5 million subscribers – of a total population of 4,4 – "the rest [non-users of mobile telecom] are either senile or infants" according to one informant) – or a significant part of a segment or a niche, such as the university welfare organizations, to whom membership is compulsory, which means that they are in a monopoly position at most university and college campuses in Norway.

In the interviews, a simple interview guide (cf. Appendix 1) was used, outlining a set of topics related to various aspects of smart card development and future diffusion. The interview guide was emailed to the informants in advance of the interviews. All the interviews, save two, were undertaken in the premises of the informants. Notes were taken during the interviews – immediately afterwards these were used to write up a report, one for each interview. In analyzing the interviews, statements and viewpoints of the informants'

were organized in a data matrix using the categories from the interview guide as an organizer. The data matrix served as a source for an empirical analysis in a separate report. Below, the main results of this report will be presented and interpreted.

Development and diffusion projects

Most of the informants interviewed were involved in projects aimed at launching smart cards, or new versions of these, some of these being large-scale projects, i.e. aimed at a nation-wide implementation. Possibly the largest of these, called “SmartKort Norge” [“SmartCard Norway”], is aimed at substituting the existing national EFT-system based on magnetic stripe cards with a smart cards based system by 2005. This project is organized by the BBS, an organization initially established as an inter-bank funds transfer and clearing-house mechanism, jointly owned by the banks in the Norwegian banking system. The BBS operates the current national magnetic stripe card based EFT-system, *BankAxept*, the system that will eventually migrate to a smart card technology platform. The cost of this migration is estimated to close to Euro 100 millions. The “SmartKort Norge”- project also serves as an umbrella for more focused projects, one of which is the “BankID”-project, which will implement a new, smart card based ID-card. Another potentially large project, called FEIDE, is a collaboration of the Norwegian State Education Loan Fund (NSELF), the university and college community and various student welfare organizations in Norway. In the telecom services, there are numerous, more diverse projects, however, most of these are based on existing smart card system in operation, i.e. SIM-cards used in the existing mobile telephone handsets. Their aim is enhancing and extending the applications on smart cards, such as development and marketing of various new payment services based on using the mobile telephone as a terminal. In addition, the mobile communications operators participate in the standardization bodies of ETSI, a mechanism important for future business case development.

A common characteristic of all these projects is implementation of applications on hardware, i.e. equipment and smart cards that have already been developed and manufactured, “not bleeding edge development” as one of the informants described this. Application design and development, system integration, business organizational implementation and marketing are perhaps the most important activities in the projects. The projects cooperate with one or more equipment manufacturers, who are candidates for supplying the project with the necessary hardware. However, application design and development is the most important activity in the projects, because these are crucial for making a business case. Thus, most of the informants used the expression “the search for a “killer application” that will rocket the smart card use”, in the way use of SMS or Internet-based banking has taken off dramatically in recent years. Thus, the focus is set on applications, a topic which will be explored further below.

The rationale for smart cards

In many of the topics elaborated by the informants, they provided viewpoints and arguments that were surprisingly similar. As will be evident later, this type of similarity indicate a common, perhaps harmonized understanding and perception of aspects related to smart card technology. However, in other areas, they were clearly divergent, making it possible to construct four distinct categories of interests in the diffusion of smart cards, i.e. reasons why smart card technology was promoted – and what kind of goals that were set for these. Informants representing different organizations and companies expressed these distinct categories of interests, i.e. they were in reality four distinct clusters of interest:

- *Financial service cluster* (7 informants) – informants working for or affiliated with smart card projects, mainly in banks or organizations controlled by the national banking community,
- *Telecom service cluster* (5 informants) – informants working for mobile telecommunications operating companies or telecommunications value-added service companies in, or affiliated with, the telecommunications sector,
- *Organizational process reengineering cluster* (4 informants) – informants working in large public or semi-public organizations, mainly at universities and colleges, organizations in the process of adopting smart card technology on a large scale for the purpose of saving costs and increasing efficiency and user flexibility.
- *Smart card technology supplier* (1 informant) – informant who represented a large smart card technology equipment manufacturer.

Financial service cluster

This first group claimed that the main reason motivating their plans for introduction of smart cards in the Norwegian banking system was due to external, international pressure. International financial service organizations such as VISA, MasterCard and Europay have adopted a smart card technology policy, in which they have embedded their own EMV-standard, and are in the process of migrating to smart card systems, gradually phasing out their present magnetic stripe cards by 2005. According to the informants, the Norwegian electronic banking and EFT-POS-system, trademark name is *BankAxept*, does not really need to "up-grade" itself to a smart card technology platform because the existing national system based on magnetic stripe card technology works well and has a high degree of security and reliability. However, in order to have international compatibility and interoperability, the existing EFT-POS-system has to migrate to the international, smart card technology platform based on the EMV-standard: "Foreigners who visit Norway and Norwegian card holders who travel abroad need terminals and cards that are compatible" was a typical explanation given. Thus, their attitude is ambivalent: On the one side, stressing the superfluousness of introducing a costly, new element in a EFT-system which works well based on the use of magnetic stripe cards, which explains a typical statement made by one of the informants:

"There is no obvious business-case for smart cards". Numerous other point of concern and doubts were added to this. On the other, more proactive side, informants point out that the bank controlled national EFT-system BankAxept is now ripe for an upgrading because the first generation of equipment and the infrastructure from the mid-1980s is becoming obsolete and worn out; an upgrading would inevitably require substantial investments in new technology anyway – so this opportunity for a shift to a smart card based technology platform should not really be considered as an unnecessary investment. In contrast to informants from the other clusters, this ambivalent attitude towards smart card technology also reflects a strong belief in the advantages of large, centralized systems, as evident in the structure of the present national EFT-system BankAxept. In fact, the informants were strong adherents (some more explicit than others) of highly centralized systems; as little as possible of the system's "intelligence" and processing power should be distributed. Some of these adherents made a point that now, when computer communication costs are negligible, the arguments from the early 1980s (when data transmission costs were high) in favor of smart cards because they could operate off-line or nearly autonomously are not relevant any more. Accordingly, only applications that would enhance "security", such as user authentication, authorization, cryptographic functions, etc. should reside in the smart card. For this reason, electronic ID and digital signature were applications that informants belonging to the financial service cluster thought could provide some justification for investments in smart card technology. This, of course, in addition to the demands from the international banking community in terms of making the national EFT-system compatible with international standards. In sum, the financial service cluster's promotion of smart card technology appears to be carefully designed as an incremental adjustment of a national EFT-system controlled by the banks – with the overriding philosophy of maintaining a highly centralized system in which the present owners would be able to maintain their positions.

Telecom service cluster

This cluster differs from the financial service cluster in a number of ways, one of which may be due the fact that the telecom community have more than ten years of experience with smart card technology, in particular because of their experience with the SIM-card in the GSM-system. A second aspect which distinguish them is a much more enthusiastic attitude towards smart card technology and its potential. These differences may be typified by the informant who claimed that: "It took us [the mobile communication operators] a long time to understand that incorporating the SIM-card in the design of the system was a stroke of genius". In this logic, the mobile telephone handset with its SIM-card reader is an ideal terminal: Most modern people carry their mobiles with them everywhere, which makes it an ubiquitous system, an advantage that other systems do not have. This, coupled with the increasing computer intelligence and processing capability of the mobile handsets, the display and numerous other features, together with sophisticated software, has transformed the handset into a miniature PC, in addition to being an ordinary, plain old telephone. The SIM-card is

also incorporated in the design of the next (third) generation mobile handsets as an integral element in the UMTS system design.

In spite of this general technological optimism in terms of the commercial potential related to smart cards in mobile communications, informants are cautious in expounding their scenarios, i.e. they are not specific as to how they envisage that these potentials may be developed. One reason for this may be the extreme competitiveness of the mobile communications service markets, in which the threshold for customers to make operator switches have become low, due to the introduction of number portability. Another, more crucial reason may be political and strategic – they do not want to provoke potential partners and competitors at an early stages in the development of new business concepts. In the field of payment services, a number of mobile operators have launched various concepts. In doing this, they have taken the step into the domain of financial services, into a territory where the banks enjoy a comfortable monopoly. Because of legal requirements, some of the operators who offer payment services have obtained a limited type of banking license from the government which allows them to handle petty cash, such as the EFT involved in payment for parking fees, vending machines, bus fares, etc. Informants belonging to the telecom service cluster claim that there are no logical or operational reasons why they should abstain from entering into full-scale EFT and related financial services, i.e. why they should abstain from providing ordinary functions of a bank. This hesitation appears to be political – informants hint to top management and corporate policy as the main restraint in this, the underlying reason is that they do not want to provoke the banking community because they are important customers, in addition they are politically powerful. Some of these informants said that they (as mobile operators) would need an alliance with a strong "merchant", typically a supermarket chain or other large retail organization. These are now in the grips of the EFT-POS-systems of the banks; some of these, such as the oil companies who have large retail outlets of gasoline stations, were even pioneers in the introduction of EFT-POS by means of magnetic stripe cards, in the mid-1980s. According to some of the telecom service cluster informants, the fees that the banks charge for EFT are out of proportion with a reasonable profit/surplus on the actual costs (one informant claimed that the ratio between charged fees and cost were 10:1), reflecting the monopolistic situation of the banks. Whatever the realism of these claims, they indicate scenarios and ambitions in the direction of competing with the banks. Others emphasized that by means of smart cards and EFT, the telecom operating companies would be able to develop and tailor business concepts that build on the unique capabilities of the mobile terminal. However, the exact specifics of these opportunities and alluded business cases were not much specified, giving impression of vagueness.

Organizational process reengineering cluster

This third group of informants are distinct from the two previous because their motives and ambitions are pragmatic and instrumental: They want to introduce smart card technology, which they already have some experience with from limited trails and experiments, because

they believe this will save the organizations for costs, i.e. smart card technology is used in an organizational cost reduction strategy. In addition, they think that smart card technology will also provide other benefits, such as increased flexibility and accountability to people and clients in the organizations. These organizations are universities and colleges, however, the Norwegian State Education Loan Fund (NSELF) a national institution for providing grants and loans to university and college students, also belongs to this cluster. This organization has plans for a large-scale introduction of smart card technology. According to their scenarios, by introducing smart card technology, the NSELF would be able to automate a substantial part of the routine, standardized paperwork involved in processing applications for loans and grants. In their plans, by using a smart card connected to the Internet, an applicant would be prompted step-by-step through an application procedure. When and if this procedure is successfully completed, the loan and grants would be transferred directly (within seconds of entering the final information) to the applicant's bank account, subsequent to signing the promissory note. The signature to be used is the applicant's digital signature residing in the smart card; the digital signature now has a legal status equivalent to an ordinary, handwritten signature. According to one of the informants, this would save NSELF large costs in terms of back-office work (routine and boring), while simultaneously increasing the level of service for the applicant, because she or he would – within seconds – know the results of the application. At present, this process takes months and causes much uncertainty to the young, prospective students, in addition to the inconvenience of first having to wait for hours in long queue in order to sign the promissory note, and, second, to wait for the funds to become available.

In contrast to the two previous clusters, the informants in this cluster think that the more applications a smart card may host, the better. However, the most important rationale for introducing smart cards on campuses and educational organizations is for economic efficiency and security reasons. In the latter, the smart card is used as a key for opening doors (entry to university buildings and rooms) and for using equipment, such as printers, terminals and copy machines. By using smart cards as keys, the system designers think that the need for guards and attendants will decrease (cost saving), while this will increase accessibility and flexibility because of increased level of self-service for the clients and users. The cards will have electronic petty cash applications so that these may be used instead of coins at campus cafeterias, laundry machines, soft-drink vending machines⁵⁸, etc.

Self-service is also the main reason why an insurance company has introduced smart card technology on a limited scale, as a trail, involving some of its largest corporate customers. These smart cards contain secure keys (cryptography) for registrations and withdrawals of employees in various pension payment programs; the smart card provides the users with a direct access to the insurance company's own computers. Both parties think that this will save paperwork-related costs. In addition, the insurance company's customers enjoy

⁵⁸ According to one informant, the Coca-Cola Company is keenly interested in this. One reason is that these types of vending machines discourage burglary, because the burglars (fast learners) know that they no longer contain coins. Also, burglary related damages to buildings decrease; at times these may be considerable.

using the direct access provided by the smart card because this gives them an increased sense of control over their pension schemes and funds. Thus, organizational process reengineering as a motive for introduction of smart card technology is not only restricted to university and college campuses, this type of rationale may also be found in commercial business organizations, i.e. smart cards as a means of reducing costs, increasing organizational efficiency and service level.

Smart card technology suppliers

Smart card technology suppliers are primarily interested in selling their goods, which in addition to smart cards and readers may encompass equipment for production of smart cards, software and services. Although only one of the informants interviewed belonged to this category (which makes it difficult to call it a cluster), the views expressed are also reflected in the industry's media exposure. Thus, they are unified in the position that smart card technology has a potential that has not been realized or fully appreciated by society. Mr. Thomas Savare of the top management in Oberthur, a large French smart card manufacturing company, proclaimed that "we are in a mature industry"⁵⁹, pointing to the fact that smart cards have been manufactured for almost twenty years, but still is far from the potential. More specifically, the industry thinks that the greatest diffusion potential is in ID-cards with embedded smart card technology; according to their estimates, only 1% of this potential smart card market has been supplied, in contrast to the GSM-market, which has a 100% saturation. In their perspective, the ID-card application of smart cards is interesting because of introduction of e-government and e-commerce, both which will require a high level of security, i.e. digital signature, cryptographies, etc., in conjunction with functions related to authentication, authorization, and non-repudiation. The security aspect has, of course, been amplified by the terrorist incidents on 11th of September 2001, however, the industry officially is cautious in its rhetoric on claiming a potential for smart cards in this connection – only making hints, such as a stronger promotion of the capabilities of biometric keys – the ultimate - as a smart card application.

Naturally, the smart card technology suppliers and manufacturers make reflections on the developmental trends of their industry and technology. In this, the notion of an emerging, dominant design is offered in predictions as to what will happen in the future: The small smart card manufacturers will gradually disappear as smart cards become based on "open platforms" operating systems. The processing and storage capabilities of the chips in smart cards will continue to increase, while simultaneously becoming more inexpensive. In this evolution, smart card technology as hardware will gradually become a commodity; instead focus will be set on applications development and system integration, i.e. a shift of emphasis from equipment to solutions.

⁵⁹ Statement made in a presentation at the *Cartes 2001* conference and exhibition in Paris, 23rd Oct 2001.

A common understanding of smart card technology

In spite of the distinct clusters of interests described above, the informants had a fairly uniform view of many significant aspects related to the role of smart card technology, its role in society and its future prospects. Below, this will be elaborated because of at least two reasons:

- A uniformity in the informants' perception of essential aspects related to smart card technology indicates that there is a broad consensus among experts in the understanding of this technology and its inherent characteristics and potential. For this reason, the clusters delineated above, i.e. where informants diverge more than anything else, may be explained in terms of different, sometimes conflicting political-economic objectives associated with how they (the informants) think smart card technology should be deployed and used,
- Secondly, homogeneous scenarios and foresights made by the type of informants interviewed are usually more accurate than non-expert predictions. The reason for this is disputed (cf. Pool 1983; Godø 2001,1993), however, the factor of self-fulfilling prophecy should not be discounted, i.e. that because new technologies are usually created for a purpose – and developed for a purpose; those who are instrumental in this are interesting as informants.

Physical cash vs. electronic cash

Among the informants, there was a surprising, somewhat puzzling, broad consensus in the perception of the future of physical cash: Coins and banknotes will not become obsolete and disappear, these will continue to exist for a long time in spite of increased use of EFT, at least for ten years in the future. Some of the informants pointed to political reasons why coins and banknotes will persist: First of all, because large groups of the population will always be incapable of using electronic means of payment, the political system cannot cut these off the monetary system. Secondly, even if capable of using electronic money, there are many people in society who prefer physical cash simply because this is a tangible type of wealth – and does not leave any electronic traces. Still others claim that physical cash, in comparison with EFT, have properties that are superior in terms of convenience in use. For this reason, coins and banknotes will stay competitive compared to EFT, at least in a number of payment niches, either related to petty cash transactions or transactions in the “informal” economic sectors of society. A typical transaction in which a banknote is exchanged for some merchandise or service may be completed swiftly, with flexibility. By comparison, EFT requires that both parties have equipment and are connected to some kind of infrastructure; the processing of the transaction, even if completed in a few seconds, is still time consuming by comparison, subject to technical mishaps.

The interpretation of this question was strategic in terms of what kind of role the informants envisage that smart card technology will have in the future: Smart cards will only

marginally compete with physical cash; instead, smart cards will compete with existing types of EFT and future business models that will require the type of EFT provided by smart cards. However, the informants were uncertain as to what kind of payment habits the young generation will drift into. Recognizing that young people's relationship to cyberspace and virtual worlds is much more "natural" compared to the older population, most of the informants believe that within one generation, when contemporary teenagers come to power, they will impose their values and habits on society. However, to what extent this will determine the role of physical cash – and that of EFT – the informants did not agree. Some point to what they claim is the *convenience of EFT* and smart cards used as money ("not having to drag around with cash in your pockets"). Others maintain that the costs and *inconvenience of EFT* will favor continued strong position of physical cash because the markets always favor low transaction costs, i.e. the markets will continue to select what economists term "efficiency". Still others claimed that one of the difficulties involved in making predictions is that the diffusion of smart card based EFT will depend on a lengthy learning process and technological evolution, which has not really started, and of which the outcome is uncertain.

The trust factor

All informants are in unison in emphasizing the importance of building trust in terms of EFT, and that this would be even more crucial for smart card technology. An important aspect of trust is security and reliability: Users of an EFT-system have to be completely confident in that the system does not try to cheat, mismanage or let unauthorized users siphon off their money or divulge information to third parties. Building trust is also described as a reciprocal relationship – the system has to make certain that it may trust its users. For this reason, according to informants, the critical function in security is authentication, procedures for authorization and non-repudiation. Some informants also include user-friendliness in the human-machine interface as essential for building trust in EFT: The user must be able to master and command the needed technology – if not, she or he will not use EFT for the management of money. In addition, the system must be fast and simple to use, both aspects make EFT vulnerable to competition from physical cash.

The high standards elaborated above as critical for building trust, most informants claimed, now exist in the national EFT-system: People – even the old generation – have a "blind trust" in these systems, they are considered completely "honest", even if many attribute them with being square-headed, rigid and inflexible. Some point to the fact that in the vicinity of ATM-machines, these are often littered with receipts that customers have thrown away or do not bother to pick up. One reason for this may be that they never control the statement of balance from the bank with the receipts or own accounts (probably they do not keep private, "shadow" accounts) – invariably because they feel absolute trust in the bank and the EFT-system. Informants belonging to the financial service cluster emphasized that this aspect, the high level of trust and confidence, had been achieved with the present magnetic stripe card

solution – which is why they feel that there is really no need for the claimed extra security offered by a migration to smart cards. Others, particularly informants belonging to the telecom service cluster, felt that trust encompasses more than reliability and security, even if these aspects are basic: It also involves diffuse aspects in relationships and identities of users vis a vis the organizations they have transactions with. They claim that the “real” trust is created when users feel that the system is an allied partner, serving proactively the user’s needs and interests. In this way of thinking, the idea of building what some informants term a “value network” is put in focus. However, in asking them to specify what this means and how they think this should be designed, they respond by describing the use of multi-application smart cards which will give the users access to a number of portals and services, which they think the user will cherish.

Biometric keys

The question of biometric keys as an application related to smart cards has been promoted as an argument for increasing the diffusion of smart cards. When asked about this (this topic was not discussed with all the informants), the response from informants were uniform in that they did not consider biometric keys to be of interest. Some of the informants claimed that they had subjected the question of biometric keys to thorough analysis and evaluation, concluding that biometric key technology still is too costly and unreliable. Others claimed that the additional security provided by a biometric key in addition to the PIN-code is marginal and would in no way justify its costs. Still others claimed that the security aspect has to be analyzed in a system perspective – that the most critical and vulnerable parts of the system must always reside in parts of the system where these may be given maximum protection. For this reason they argued in favor of centralized systems, typically the viewpoint of the financial service cluster. Accordingly, highly distributed systems (e.g. having numerous applications on smart cards and peripherals) are more risk exposed – in addition to aspects related to economy of scale, which they claim is more difficult to obtain in distributed systems.

Smart card technology standards

Most of the informants⁶⁰ claimed that the ISO 7816 standard for smart cards is solid, i.e. that this standard is recognized as firmly established and that no contesting design exist or are likely to emerge in the foreseeable future. In addition, informants belonging to the telecom service cluster made almost identical statements regarding the ETSI-standards related to smart cards, i.e. GSM 11.11 and GSM 11.14, which define the SIM-card. However, in terms of vertical standards and operating systems in smart cards, the informants were more split. One group of informants claimed that the operating system was irrelevant, because the EMV-

⁶⁰ I.e. those who felt that they had an opinion on this; two did not go beyond stating the importance of adhering to standards and “open systems.

standard is most important. In contrast, other claimed that the JavaCard operating system was best, because it is convenient for programming applications, especially multi-applications. Still others, claimed that MULTOS was best for smart card applications requiring a high level of security and capability of functioning securely in an off-line environment, independent of systems connected to banks, just like the use of physical cash. Whereas MULTOS was a favorite among informants affiliated with the telecom service cluster, the EMV-standard had, not surprisingly, most support among informants in the financial service cluster. The political dimension in these viewpoints is obvious: Adherents of the MULTOS standard want a system that is independent of the EFT-system controlled by the banks – the EMV-adherents want standards that will maintain the existing centralized EFT-system.

In the broader discussion with informants on the global issue of smart card technology standards, why Europeans dominate this, numerous informants compared the banking system of USA with Europe. In this, they pointed to cultural and structural idiosyncrasies of USA's banking systems, in which the use of paper checks still have a dominant position as the means of fund transfer: "The Americans are hopelessly antiquated in this" was a typical comment made by informants who claimed that this, in contrast to the national and European scene, was due to the sector's inability to cooperate in developing joint EFT-systems.

Multi-application smart cards

In the international smart card development community⁶¹ there are groups which believe that designing multi-application smart cards will make smart card technology more attractive to users, because then a single card may be used for many functions, or what some call "a generic access token". In addition, they claim that the cost of each application will decrease if many can share one card, i.e. a cost sharing strategy. Naturally, this strategy is highly endorsed and promoted by manufacturers and suppliers, who claim that their product is ideal for multi-applications. One of these, Sun Microsystems, is promoting its operating system JavaCard in an attempt to make this a de facto standard for smart card software engineering. In the interviews, the response to this topic was surprising: Apart from the informants associated with the organizational process reengineering cluster, all the other informants were skeptical to the idea of multi-application smart cards. The main reason for this is based on their understanding of what a multi-application smart card is – a smart card in which a number of applications provided by different companies and organizations. In claiming that multi-application smart cards are unattractive, most of the skeptics pointed to the question of ownership, administration and operation/maintenance of the smart card as the problem. For this reason, some of the informants claimed that instead of lower costs, a multi-application smart card, if feasible at all, would probably cause cost escalation because of increased coordination costs involved when many actors try to cooperate in fitting numerous

⁶¹ Cf.: <http://eeurope-smartcards.org/tb7/htm>, which provides general information on EU's initiative with multi-application smart cards, and <http://www.mta.fr/tb7page.htm> for more specific information.

applications into a single card. Some claimed that maintenance, especially up-grading, of multi-application smart cards could easily develop into a costly management nightmare: How do you deal with a situation when a card is lost or stolen, or how do you deal with a card-holder who is black-listed by one of the application owners, but not the others?

In contrast, the informants who were positive to multi-application cards pointed to their own experience, which they summed up as: The more applications a card can host, the better for all parties. The main reason for this is that the users like having numerous applications on a single card; this is convenient for them. They also claimed that multi-applications in fact lowers the cost of each application and that this type of cost sharing strategy is feasible and convenient. These attitudes and experiences contradict skeptical informants' views, which one may be tempted to interpret as being motivated more by commercial, strategic considerations than anything else.

Technological systems, competition and diffusion

In a technology diffusion perspective, one may claim that the smart card already has attained a high degree of diffusion, mainly because of its use as the SIM-card in the GSM mobile communication system. The telecommunications related use of smart cards account for approximately 70% of its present use. The diffusion of smart cards is closely related to the growth of specific technological systems, dependent on the designers' and owners' choice of overall system architecture, its various elements and components – and how the system is set to operate. Thus, it was initially claimed that the diffusion of smart cards in many ways resemble Rogers' category of *authority innovation-decision*, because of all the large and small decisions taken by system designers (a comparatively small number of people) on how the system should be constructed; however strategic, the smart card is but one of a number of elements. The individual user's relationship may be labeled, according to Rogers, as a *contingent innovation-decision*, or, to put this another way, as a "take-it-or-leave-it"-strategy. As evident from the survey of major smart card project leaders and decision makers presented earlier, the motives and dynamics for introducing smart cards differ, reflecting a divergence of ideas of what a smart card is – and how they want the smart card to work. Simultaneously, they were surprisingly unison on a number of important topics related to smart cards, such as the stability of present standards, the continued existence of physical cash (banknotes and coins), etc.

In the analysis of the various opinions expressed by informants, it was possible to discern four distinct groups, or clusters, each cluster reflecting disparate interests in the introduction and diffusion of smart card technology. In the financial service cluster, although their aim is a full-fledged, nation-wide transition from magnetic stripe cards to smart cards by 2005, the informants were clearly ambivalent, claiming that this transition was more or less forced upon them by influential actors in the international financial and banking community. Some of the older informant belonging to this cluster pointed to a heated, bitter controversy in the national banking community in the mid-1980s, between adherents of a national system

based on smart cards and a rival faction of magnetic stripe card adherents. The latter faction, with close ties to the saving banks system, finally won, because they successfully argued that the cost of a smart cards based system would be large and that smart cards were technologically risky. The subsequent establishment of the national EFT-POS system BankAcept was based on magnetic stripe cards, i.e. it simultaneously became a de facto monopoly. Now, almost twenty years afterwards, the “victors” (those who advocated the magnetic stripe cards solution in the controversy in the 1980s) point to the success of BankAcept as the proof that they were right. This may explain their ambivalence to the transition to smart cards, because, as some of them claim, the technical-economic rationale for smart cards is even weaker now than in the 1980s – there is still no convincing business case for smart cards, they claim.

In contrast, the informants from the telecom service cluster argue for the superiority of smart cards, i.e. the geniality of integrating the smart card (SIM-card) in the design of GSM, alluding to its contribution to the success of GSM. Their attitude to smart cards (SIM-cards) is that this, combined with the mobile telephone handset, is an ideal terminal for a multitude of potential applications. Some of these, such as the petty cash application, have cautiously been launched for paying parking-lot fees and similar petty cash payment functions, in which the mobile telephone handset becomes an EFT-POS-terminal. However, the ambitions are to move into new areas of payment in order to become an alternative to the EFT-POS-systems monopolized by the banking community. They think that they should be able to compete with the banks in this because of a number of advantages, one of which is price. In their mode of thinking, the payment application, however strategic and essential, is just one of numerous value-added services which constitute future business cases. Whereas the mode of thinking in the financial service cluster is focused on promoting services to users in their centralized systems, the telecom service cluster is more focused on solutions that will increase the use of their networks. For this reason, they favor distributed solutions, and they think the use of smart cards will serve this purpose better than other, alternative solutions.

Broadly, one may summarize the strategy of the financial service cluster as defensive because its overarching motive seems to be retaining its present dominance over the flow of money in society by means of extending its centralized system. In contrast, the telecom service cluster is more offensive, searching for new ways to develop what they believe are interesting business potentials associated with a combination of their networks and smart cards. This, if successful, could grow and become a serious competitor to the hegemony of the banking sector. In the organizational process reengineering cluster, cost reductions and increasing operational service level and flexibility within their organizations is the main impetus for introducing smart cards. However, the technological potential in the smart cards may encourage its system designers to provide applications competing with other systems – as evident in their open attitude towards multi-application smart cards. All of these systems have in common that the smart card is used as a key, first of all as a means of accessing a system, but, in addition, to host other applications. The extent and scope in terms of what kind and how these applications are implemented differentiates the systems. Technologically, these smart card keys are homogeneous – all of them comply to the specifications set in the ISO

7816 standard and other standards that contribute to increase harmonization and interoperability, typically illustrated by the concept of “open platform”. This developmental trend is in accordance with explanations of how a *dominant design* becomes established (cf. Abernathy and Clark 1985; Utterbach and Suarez 1993; Lee, O'Neal et al. 1995), however, the systems in which these are incorporated are designed for different aims and interests, as explained above; potentially they may even become competitors. The strategic factor in this is to what extent the different smart card based systems encroach or slide into the other's territories. In this, the control of EFT seems to be strategic.

In a technology diffusion perspective, the aggregate level of smart cards (its total “population”) will probably continue to increase, possibly following the “normal” pattern in a S-shaped curve, as this passes the point of “critical mass”. The reason why this may be predicted with some certainty is that decisions to adopt smart card technology are of the type Rogers called an authority innovation-decision: The system designers and owners decide – the users do not have any choice or direct influence on how the system is designed, he or she is given a “take-it-or-leave-it”-option, what Rogers called a contingent innovation-decision. Although this gives the single user little power, the sum of what all users or potential adapters choose is crucial for the innovation-diffusion – and for the success or failure of the system in which this technology is embedded. Thus, it would perhaps be more appropriate to qualify Rogers' terminology: Making decisions on a system level, the growth of smart card technology is based on *market-oriented* authority innovation-decisions, which is complementary to, and interacts with, *system-dependent* contingent innovation-decisions, often in conjunction with other types of innovation-decisions.

As the different clusters start to offer applications that other systems will provide as basic, possibly instigating competition between different systems, the power of the user may increase because he or she is put in a position where choice of systems becomes real alternatives. From the analysis, it is evident that the different clusters pursue their own strategies, however, in a technology innovation diffusion perspective, the landscape that emerges becomes complex and immensely large. Thus, all of the types of decisions that Rogers have categorized to some extent explain parts of the picture, making the sum of explanations murky and unsatisfactory. For this reason, it is tempting to agree with Bruno Latour's criticism (Latour 1987) of innovation diffusion theory, such as expounded by Rogers, which Latour depicts as superficial, because it describes what is represented in the smooth S-shaped growth curved, i.e. diffusion is a predictable, frictionless development following a pattern of ordered regularity. In Latour's explanation, which he uses to promote his own actor-network theory (ANT), he depicts the diffusion of innovations as chaotic and thorny, with abundance of controversies, conflicts, negotiations, compromises and transient, often shaky, alliances. Accordingly, Latour claims that a more fertile approach to explaining the emergence and dissemination of new technology is to analyze this as a series of numbered (1-5) *translation processes*. In Latour's scheme, the ultimate goal for a new technology is to successfully pass what he calls “translation five”, i.e. achieving a state in which the technology has become indispensable ((Latour 1987, p. 119-120). Prior to this, in the four previous translations, the initial creation of the novelty is usually modified (if it survives at

all) in all the translations. For the inventor/innovator, according to Latour (Latour 1987, p. 108), his best strategy is to do two things simultaneously:

- *enroll others*, so that they participate in the creation and realization of the novelty,
- *control their behavior*, in order to make their actions predictable.

The difficulty in replicating Latour's analytical strategy is the sheer complexity, temporal dimension and size involved in the emergence of large technological systems, such as the smart card based technological system and the keys these embed. However, the face value of Latour's concept of "translation five" in which the technological novelty becomes indispensable may seem as an accurate characteristic of the current status of smart card technology in Europe. In fact, an obvious explanation of the financial service cluster's migration to a smart cards based system could be interpreted as smart cards are in the process of becoming indispensable. The reason why this has happened is not primarily technological – it is political: The Norwegian banking system has been compelled to migrate to a smart card based EFT-POS-system due to decisions taken by powerful organizations outside the sphere of influence of the Norwegian banking system. They have to accommodate to these decisions, they feel, both in terms of ensuring compatibility to the new standards (hence technological change to smart cards) and in order to maintain its hegemony in a highly centralized EFT-system. Thus, one may claim that the act of incorporating the smart card in the system design, as done in the GSM-system early in its development, is what makes the technology indispensable, even if mobile handset manufacturers are attempting to remove this from the design. However complex, these types of decisions are taken at one point in time, usually by a few persons, in what Rogers would call an authority innovation-decision and similar to Latour's concept of translation five. If this is admitted as a legitimate interpretation, the difference in explanations between Rogers and Latour are really minor, more a question of rhetorical style and taxonomy – hence translation may make the explanations homogeneous. Of course, the ultimate success of a new technology will be decided by the users and the markets – if they accept, or still better, if they demand with a deep desire, or reject/ignore the novelties promoted by representatives of the technological system. As pointed out earlier, because smart cards are integrated in the system, the user will probably not care much as to how and why a smart card works; he or she will be interested in the goods and services that the card will enable or access – what is inside a card is for them just a "black-box", something which will give access to the system if the right PIN-code is entered.

6 Electronic money and smart cards

Introduction: The problem of electronic money

"The killer application for electronic networks isn't video on demand. It's going to hit you where it really matters – in your wallet. It's not only going to revolutionize the Net, it will change the global economy". This is quoted from the introduction of an article written by Steven Levy in the *Wired Magazine*, in December 1994.⁶² In the article, what he called "the next great leap of the digital age", smart cards would substitute physical cash by using cryptographically sealed digital streams. One reason for making this strong prediction was the research he apparently had undertaken in the mathematically oriented community of developers of cryptography based on asymmetric keys, or PKI – Public Key Infrastructure. In particular, Steven Levy gives the impression of being fascinated by the ideas of David Chaum, who at that time had established an up-start company called DigiCash in Amsterdam. The business idea of DigiCash was based on patents that Chaum had obtained for his inventions in cryptography, which would make anonymous electronic cash possible. Another reason for Levy's prediction may have been his conviction that cyberspace was "...desperate for immediate implementation of the digital equivalent" of physical cash. This belief, that the lack of an adequate electronic means of payment equivalent to physical cash, represented (and still represents) a barrier for the development of ICT, is a belief he shares with many analysts, players and observers.

Seven years later, just prior to the first bursts of the dotcom-bubbles and the 11th September 2001 incident, an article was published in the same magazine as that Levy had published in, the *Wired Magazine*, describing the failure of the companies that had attempted to develop and commercialize various types of digital money: "The electronic cash landscape is littered with looted corpses of companies that tried and failed to compete with credit cards for online purchases. True digital cash that's as anonymous, as privacy-protected and cheap as the humble greenback seems to be one of those technologies that pundits laud and technologist adore, but markets stubbornly fail to adopt".⁶³ DigiCash had gone bankrupt in 1998, others, such as eCash and CyberCash, if not bankrupt, were not very successful. This development has puzzled many analysts, because it is so counterintuitive to what they expected, i.e. what seemed so obvious, so promising in terms of a development potential for meeting a very latent, pent-up demand. In this, the role of smart cards, with its potential for embedding sophisticated cryptographic software, was expected to have a leading role. Because of these failures, Chares Goldfinger, in an analysis of financial applications of smart cards, asks: "...are there some fundamental problems with current concepts and approaches to

⁶² "E-Money (That's What I Want)" – downloaded from:
www.wired.com/wired/archive/2.12/emoney_pr.html

⁶³ "Digging Those DigiCash Blues" by Declan McCullagh, downloaded from:
www.wired.com/news/print/0,1294,44507,00.html

the [smart cards based] electronic purse, problems which may require radical rethinking of these concepts and approaches?"⁶⁴. In trying to answer this question, which without doubt has been asked by almost all in the smart card industry, he points to all the aspects that the informants presented in last chapter identified as challenging, e.g.: lack of business case, high costs, etc. In spite of this, he presents a remarkable and surprising conclusion/recommendation: That smart cards with financial applications combined with the mobile communication system GSM is the most promising avenue for development in the future, at least in Europe. This is almost identical to the aspirations of some of the mobile telecommunication operators presented in the last chapter. In spite of this conclusion and the reasons for reaching this, which are not so clear, the question he asks is perhaps the most significant. The problems may be similar to those encountered in the early days of computers, right after WWII, when computer scientists tried to design translation machines: Initially, they thought that this was just a question of making dictionary files, e.g. translating English, word by word, to Russian. The results were, of course, absurd, however, this failure made apparent some of the complexities of "natural" language. Following this, one may ask: Are the difficulties with digital cash and the technological solutions designed due to misconceptions or superficial understanding of value – and the way society regulates values and its circulation? In our thinking about money – we think of this in terms of cash in our purse or the credit/debit of our accounts in the bank. Obviously, trying to answer a question like this is almost impossible, however, discussing some aspects of this – and the role of virtual keys – may be legitimate. This will be attempted in the following, first by giving an account of the status and role of physical cash and electronic payment in society. This will be based on data from Norway, from the Central Bank of Norway. Following this, the question what is really money, will be asked and discussed in terms of Georg Simmel's theories of this. Finally, this will be discussed in terms of smart card development.

Cash and electronic payment in Norway

According to the year 2000 annual report on the national payment system published by the Central Bank of Norway, Norway is emerging as a "cashless society", because the use of physical, "real" cash (i.e. coins and banknotes) has diminished simultaneously as various types of electronic payment instruments have taken a dominant position⁶⁵. The value of the remaining physical cash, as a proportion of the country's GNP was in 2000 less than 4%. This share was approximately 8% in 1980, i.e. prior to the introduction of electronic means of

⁶⁴ Charles Goldfinger, "Economics of financial applications of the smart card: A summary overview", downloaded from: <http://europa.eu.ist/ISPO/fiwig/archives/steering/fasc.htm>

⁶⁵ Cf. Norges Bank (Central Bank of Norway), *Årsrapport om betalingsformidling 2000* [Annual report on payments 2000], Oslo, May 2001, p. 6-7.

payment such as EFTPOS⁶⁶. In "over-the-counter"-type of payments, such as purchase of retail goods in ordinary stores or paying for restaurant bills, less than 50% of these transactions now (2000) involve the use of physical cash, whereas this figure was about 90% in 1980. As an extrapolation of this development, the analysts of the Central Bank of Norway predict that in 2015, this share will be approximately 5%. This developmental trend is typical in most OECD member countries, however, with some distinct national exceptions, such as Japan, which has a surprisingly low dissemination of EFTPOS-terminals, and USA, in which cheques still hold a strong position as a means of non-cash payment. These national idiosyncrasies are due to institutional structures that reflect that the banking systems have failed to cooperate on providing the needed infrastructure.

The aforementioned report from the Central Bank of Norway presents an exhibit⁶⁷ that shows that during the 1990s, the share of cashless, electronic payment transactions increased in a number of OECD member countries, so that the average share of this of all transactions being 78% in 1998. One may reasonably expect that this trend will continue, i.e. the migration of payment towards electronic media in which the share of physical cash will diminish even further in this process of substitution. In this process, the monetary value of each individual transaction will probably decrease as the number of electronic transactions increase, because these increasingly will substitute petty cash functions, such as payment for bus and taxi fares, newspapers, small amounts of groceries, snacks, refreshments consumed on the spot, etc. Based on extrapolations of recent trends, one may predict that at some point during the next 10 to 15 years physical cash will disappear, as its share of payments in transactions involving small amounts becomes almost zero. However, there are numerous doubts to the likelihood of this trajectory for a number of reasons, which now will be discussed, because in these the role of keys and locks also play a role.

Even developers of electronic payment systems, people who have a professional interest (which often overlaps with a private, pecuniary or ideological, interest) in the promotion of electronic means of payment such as those based on smart cards, doubt or are uncertain with regard to the prospects of a completely cashless society. A number of reasons support this belief: Physical cash, they claim, is versatile and flexible compared to electronic means of payment because its use does not require a technical infrastructure or specialized terminals at the points of transactions, at the numerous points where people interact and trade⁶⁸. For this reason, physical cash is also robust; transactions involving cash do not depend on an outside technical system, which eliminates vulnerabilities to technical system and terminal failures, which is always a risk in the use of electronic means of payment. Because the size and weight of physical cash is comparatively small (e.g. a typical, clean

⁶⁶ EFTPOS = electronic funds transfer point of sale, a term used to designate the type of terminal that will accept electronic "plastic money" (usually magnetic stripe debit cards) as payment.

⁶⁷ Figure 1.2 in the report, cf. note 1 above.

⁶⁸ Physical cash require infrastructure and institutions, such as central banks that provide coins and banknotes – and control and maintain the circulation of cash, they also require distribution channels, protection of laws that forbids copying (counterfeit) and the monopoly of central banks, etc.

banknote weighs about 0,8 g – coins are heavier, however, even physically large copper coins weigh less than 10 g) – they are easily carried around⁶⁹.

These factors make use of physical cash inexpensive for users because they do not require investments in special infrastructure and do not incur extra operational costs (even if these have become much lower during the last decade) – the system costs of physical cash, which are high, are carried by "others" (i.e. society) and charged indirectly because it is difficult or impossible to charge these costs at points of transactions. During transactions which involve physical cash, the operations may be rapid: In a typical transaction, the time consumed as a customer hands over the coins or banknotes, and the cashier completes the transaction by handing over the change (sometimes with a receipt), is undertaken in a few seconds, which usually is much faster than a transaction in which EFTPOS-terminals are used. In the latter, both the cashier and the customer have to wait for the systems to process the transaction, i.e. the time expended in authentication of the user (which also involves entry of PIN-code) and authorization of the transaction.

In addition to these aspects, some analysts point to the fact that physical cash is prevalent in the "informal" economic systems of society, as a means of private storage of value and for transactions in the "unregistered" part of the economy, as explained in the annual report from the Central Bank of Norway. In this, banknotes with the highest denominations are popular – denominations with a value above what most people consider as petty, everyday cash. This type of cash usually irritates cashiers at stores because these tend to "rob" them of all their change. Although empirical evidence is scarce, the popularity of physical cash, in particular banknotes with high denominations, in the "unregistered" part of the economy may be attributed to their anonymity – the banknotes are "dumb" and "deaf", they lack the built-in memory and input device capable of recording its own circulation and use; they do not leave any telltale electronic traces which will give information as to their movements⁷⁰. In the future, one may imagine that banknotes, in order to discourage counterfeit⁷¹, may become less anonymous, being equipped with bar codes or even integrated circuits.

⁶⁹ Of course, there are numerous cases in which physical cash have become bulky, as evident during periods of galloping super-inflation, such as in Germany during the Weimar republic in the 1920s. At one point, a whole wheelbarrow of banknotes were required for buying a bread. In his autobiography, *Die Welt von Gestern: Erinnerungen eines Europäers* (1955), Stephan Zweig gives a vivid account of the hardships this caused in his daily life in the Weimar republic.

⁷⁰ All banknotes are given unique identity by the issuer, the central banks, usually a serial number combined with the year it was issued.

⁷¹ According to an article in *Aftenposten's* Internet edition, 25 March 2002, the number of counterfeit cases almost doubled from 1998 to 2001 in Norway. According to one police officer interviewed in the article, "clean" youngsters who used their private scanners, PCs and color-printers to make the fake banknotes, i.e. juvenile delinquency, not organized crime, committed many of the counterfeits. The police officer claimed that the youngsters do not understand the serious implications of their activities. The US dollar banknotes have a notorious record for being easy to counterfeit. In order to counteract counterfeits, central banks are

The anonymity of cash may explain a peculiar and paradoxical phenomenon observed in Norway: According to the Central Bank of Norway, in spite of the increasing use of electronic means of payment as explained earlier, the amount and value of physical cash held by the public has also increased⁷². As this does not make sense, analysts at the Central Bank of Norway have attempted to estimate to what extent this may be attributed to the "unregistered" economy. According to their estimates, which is based on a "residual" approach, i.e. what is inexplicable after subtracting the amount of cash-based payments from the total amount of cash circulating in the "legitimate" part of the economy, there is a residual of approximately NOK 27 billion worth in banknotes which is unaccountable. Although some of this may be attributed to irrational savings (in particular old people who distrust banks and prefer to hide their savings at home), the analysts claim that a substantial part of these belong to the "black" economy of society, i.e. the banknotes are used as payment for avoiding taxation, or because the transactions involved are illegal or morally dubious, such as narcotics, etc. Accordingly, the analysts claim that the figure, NOK 27 billions, correlate with the estimates made by the Norwegian Tax Administration, in which the illegal (tax avoiding) economy is estimated to constitute about 10% of the GNP of Norway, i.e. approximately NOK 140 billion in year 2000. The inference from comparing these two figures is that the flow of currency in the "unregistered" economy is slow, about 1/10th of the speed in the legitimate economic sectors. As noted earlier, banknotes with a high denomination are favored in this "black" economy. Thus one may reasonably guess that in the unregistered economy, the numbers of transactions are comparatively few, and that each transaction involves payment of fairly high amounts. A typical transaction of this kind would be the well known type payment to a carpenter or plumber, who gives his or her customer a "discount" (equal to the VAT or other taxes) for not providing a receipt for the payment, or the payment of narcotics, prostitution, illegal gambling, etc. All these transactions usually involve comparatively large amounts of cash, for which banknotes with high denominations are used – often these notes circulate in their own spheres. Re-entry of these banknotes into the official economic system may be associated with risks, as evident in the phenomenon of money "laundry". Still, because of the illegalness of these activities, the estimates and explanations presented above are conjectures, the facts as the banknotes are in the dark.

The persistence of physical cash

Thus, there seem to be at least three, somewhat overlapping reasons why physical cash persist, in spite of a strong tendency and migration towards electronic means of payment: The cost of making electronic cash universal is still too high for a number of petty cash transactions. In particular, costs related to building an infrastructure, development of

issuing new bank notes with sophisticated water marks, security silver threads and embossments, in addition to using colors and graphical details that make copying more difficult.

⁷² Cf. "Kontanter – mest til svart bruk?", Sparebankbladet, nr. 11/2001 ["Cash – mostly used for black markets?"]; article in the journal of the Federation of Saving Banks of Norway, no. 11/2001]

applications, management and processing costs, etc. are considered too high to be of interest according to developers of electronic cash – for this reason they are not able to get a clear picture of a business case or model that may justify these types of investments.

Physical cash have inherent functional properties that compare well with electronic means of payment, in terms of mobility, versatility and flexibility. Thus, for numerous types of payment, using physical cash are fast, secure and convenient – i.e. has a clear advantage in comparison with existing electronic means of payment.

Physical cash is “mute”, it does not possess any inherent memory or register as to its movements, which explains why this type of payment is favored in the “unregistered” sectors of the economy. In these types of transactions, the users want as much privacy as possible. The exact reasons for this are not well known. However, most people have some experience with this sector of the economy, for which reason one may safely assume that tax evasion and trade in illegal goods and services are probable explanations for why banknotes are favored as means of payment. An additional reason may be distrust of banks, especially some older people who are suspicious of banks and authorities seem to prefer private storage of their cash fortunes, hidden in their homes, etc.

Of these three reasons, the persistence of physical cash related to the “unregistered” sectors of the economy is perhaps the most elusive. One may imagine that if technical countermeasures are introduced so that banknotes become less anonymous, this sector will act like a balloon being “strangled”, it will adopt other means of payment that retain the anonymity of today’s cash, even if these are not as convenient. One may even imagine the evolution of an “unregistered” electronic economy, an economy which operates with its own banks, perhaps in collaboration with the numerous, secretive “offshore” banks that exist today (Cayman Islands, etc). A different scenario is the development or re-emergence of various types of barter and swapping-schemes aligned to the “official” economy, based on the use of IOUs. In sum, there is no reason to expect the “unregistered” economy to disappear as long as this provide business opportunities for those who dare and care. Thus, the real challenge to physical money is set by the first two aspects above, related to the comparative advantage of physical cash in comparison with electronic means of payment. However, in order to explore this topic further, some fundamental questions related to the nature of money need to be discussed.

The nature of money

As with the discussion of keys and locks, the phenomenon of money needs to be analyzed with a focus on its existence in physical, material and electronic versions. In theory, the two versions are interchangeable and thus equivalent, which explains why many economists think of these as identical, i.e. that the distinction is trivial because these are technical implementations, merely two slightly different instruments that are functionally equivalent. In this perspective, physical cash and electronic money are identical because their main purpose is transportation of values, i.e. basically both are essentially information. However, as evident

in the political resistance against the introduction of the new currency Euro, which was hotly debated in 1998 and 1999, approximately 70% of Germans were opposed to the idea of abandoning the German currency Mark in favor of the Euro. According to analysts, the main reason for this was national identity, i.e. that the majority of Germans felt that the introduction of the Euro would take away something that truly belonged only to Germans⁷³. Technically, such sentiments as national identity associated with a particular currency is irrational, however, similar sentiments are prevalent in the UK and USA in terms of resistance to the introduction of the metric system for weights, measurements, temperature, etc., i.e. abandoning one convention in favor of another is not as simple as changing a toothbrush or a shirt. Of course, psychological factors and sentimentality probably play a role, however, the tacit knowledge aspect related to various conventions of measurements should not be underestimated. Thus the term “inch” carries extra meaning, a person familiar with this will be able to give a fairly exact description of the unit, whereas “centimeter” is something abstract, unfamiliar. Furthermore, references, metaphors, rhetorical terms, etc. in the language use these units, such as expressions “not one inch”, or even verbs, such as “the cars inched along the motorway in the traffic jam”. These few samples show that much more is at stake than the instrumentality of units and their nomenclature. In order to focus on this, the main emphasis in the following will be on money, following Georg Simmel’s claim that “..the fact that two people exchange their products is by no means simply an economic fact”– i.e. that beneath the surface level of economic affairs, it may be possible to derive “..the ultimate values and things of importance in all that is human” (Simmel 2001, p. 55).

The idea of money

The most fundamental, yet elusive aspect related to money is the phenomenon of *value*. According to Simmel, this question is unanswerable, thus it is not possible to give value a positive, substantial definition. However, value is not an inherent aspect of an object, rather a subjective judgment, thus a quality of those who make judgments (Simmel 2001, p.65). Thus Simmel defines what is valuable operationally as those objects that “..resist our desire to possess them” (Simmel 2001, p. 67) – the higher the resistance and/or desire, the more valuable. By this, Simmel establishes value as a cultural-psychological phenomenon, closely related to the relative scarcity or abundance of something. Following this, Simmel defines money as “..simply “that which is valuable”, and economic value means “to be exchangeable for something else” (Simmel 2001, p. 121). For this reason he claims that money is a medium

⁷³ Cf. “Currency Conflict Mirrors Europe’s Shifting Politics”, by William Drozdika, Washington Post Foreign Service, 17 Feb 1998, page A 08, downloaded from www.washingtonpost.com. For similar reasons, a majority of Danes voted against Denmark’s entry into the Euro-currency in a referendum. Subsequent to this defeat, the Swedish government decided to cancel a similar referendum, because opinion polls indicated a high resistance in the Swedish population. Apart from Denmark, none of the European countries that entered the Euro-currency system held referendums on this question, however, opinion polls indicated strong anti-Euro sentiments in most countries, in particular in countries “north of the Alps”.

for articulating the relativity of values that are attached to various objects. Thus, he claims that:

“To the extent that money expresses the value relationship between goods, measure them and facilitates their exchange, it enters the world of useful goods as a power of entirely different origin, either as an abstract system of measurement or as a means of exchange which moves between tangible objects as does ether between objects possessing weights.” (Simmel 2001, p. 122).

For this reason Simmel claims that money needs to have a material and specific value in itself because of its “yardstick”-function: Because money “measures” value, it must have some kind of value itself, just as other types of measuring devices must have a calibration point with characteristics similar to the objects of measurement; weights must weigh something in order to measure weights, the measurement of length must have some physical extensions in space, etc. However, this is not so obvious with money, because a process of increasing abstraction is involved, in which money has developed as a means of expressing the relative value of objects, independent of its own intrinsic value. Thus, paper money initially evolved as tokens representing specific material values, usually units of gold, because of the convenience in terms of weight of paper compared to gold. As money has evolved, the links to something substantial have gradually become weaker⁷⁴. The direction of this development is increased symbolism in the expression of values, i.e. that the values are “incarnated” in symbols as they have evolved to more abstract media (Simmel 2001, p. 149). However, according to Simmel, this trajectory toward abstraction has to stop at some point, because if all relationships to physical substance are cut off, i.e. if money becomes completely abstract and information-based, it will simultaneously dissolve itself as being money. This claim, as Simmel himself points out, is in contradiction with his own definition of money as having “..no intrinsic value of its own”, i.e. as merely being a medium which will enable comparison of different values in order to make trade and circulation of goods and service provision possible. However, his arguments for the claim that in spite of this, value must in some way be embedded in a material substance which then becomes valuable, is subtle, almost psychological: He explains that “..all elements in life depends upon the occurrence of opposing elements” (Simmel 2001, p. 166), i.e. if money severs all its bonds to something material that is considered valuable, then historical evidence proves contrary – money must have some intrinsic value.

In addition to this, Simmel’s explanations of money include other factors, such as the institutionalization of money value: “When barter is replaced by money transactions a third factor is introduced between the two parties: the community as a whole, which provides a real value corresponding to money” (Simmel 2001, p. 177). In making this point, he takes note of what he claims Adam Smith once wrote (Simmel never uses references or give exact information about his sources), that gold and silver are merely tools, similar to kitchen utensils, i.e. that increasing the amount of gold and silver does not contribute more to the

⁷⁴ In fact, the “gold standard” was abandoned in 1972 subsequent to the breakdown of the so-called Bretton Woods-system, in which the value of national currencies and the rate of exchange, were negotiated based on nations’ possession of gold.

wealth of society, no more than the increase of kitchen utensils will provide more food (Simmel 2001, p.173). This point is in accordance with his basic claim that money does not have any inherent value. Still, he struggles with how to explain why money or whatever object that represents this will be considered valuable. Thus, he invokes the term “dual nature of money” – that money on the one hand is “...a concrete and valued substance”, but that it is simultaneously “...something that owes its significance to the complete dissolution of substance into motion and function”, because money is the “..reification of exchange among people, the embodiment of a pure function” (Simmel 2001, p. 176). Perhaps this dual nature, which Simmel struggled with because it may have been painfully illogical to put this into writing, does indeed make sense, as evident in the problems encountered by people and companies that have attempted to create anonymous electronic cash based on smart card technology.

The role of money in society

Whereas the logics of Simmel’s explanations of money and value as a phenomenon may at times seem inconsistent or tautological, as Simmel himself has admitted⁷⁵, he is more explicit in elaborating the role of money in modern society. His basic claim is that as money has become generalized, being used for a totality of purposes, this has made money the ordering principle and mechanism of modern society. For which he endorsed a contemporary thinker who claimed “Money is the secular God of the World” (Simmel 2001, p. 238). The significance of money is evident in numerous psychosocial effects involved in human interaction because of the pervasiveness of money. Accordingly, money gives exponential growth in power and prestige; the quantity of money causes qualitative differentiations. Money provides a new type of freedom of choice, however, Simmel qualifies this by claiming that this implies changes in the types of obligations of an individual: Whereas the introduction of money liberates an individual of personal bonds (such as in feudalism), it simultaneously makes the individual dependent on others in a different way: In money-based modern societies, the liberated individual will become dependent on an increasing number of individuals, this reflecting the increased division of labor and specialization made possible by money, i.e. the increasing complexity of society. Thus he claims “Money has provided us with the sole possibility for uniting people while excluding everything personal and specific” (Simmel 2001, p. 345). Although this may represent freedom, it is sterile, because increasingly, the human content of interactions diminish. Following this, it may not come as a surprise that Simmel considers the slot machine as the “..ultimate example of the mechanical character of modern economy” (Simmel 2001, p. 460), because this completely eliminates the human relationship, as this is substituted by a mechanical device. This, combined with

⁷⁵ In the “Afterword: The Constitution of the Text”, written by the translators Tom Bottomore and David Frisby in the 1990 English edition of Simmel’s *Philosophy of money*, they provide evidence that this also constituted the greatest difficulty for Simmel himself when he wrote the book (cf. p. 518). This is based on information in a letter that Simmel wrote to a friend, in May 1898.

urbanization, where an “..enormous amount of people, sensitive and nervous people” demand a psychological distance, because otherwise communication would be “unbearable” – this making objectification of social relationships necessary, in order to create inner boundaries and reserves (Simmel 2001, p. 477). In Simmel’s mind, urbanization, money and modernization are intimately interrelated, which he depicts as a vicious misalliance, “..in the instability and helplessness that manifests itself as the tumult of the metropolis, as the mania for traveling, as the wild pursuit of competition, and as the typically modern disloyalty with regard to taste, style, opinions and personal relationships” (Simmel 2001, p. 484).

To simplify Simmel’s verbose explications, his basic claim is that whereas modern money contributes significantly, possibly even essential for the liberation of individuals from ancient social bonds and institutions by eliminating the obligations associated with these, money also creates alienation associated with freedom. Of course, the transition to a money economy requires new institutions – which in turn contributes to the emergence of modern society. Modern society, in turn, is evolving towards increased complexity due to increased division of labor, specialization and increased geographical convergence of economic systems, i.e. what is now called globalization. Thus, the moral and normative undertone in Simmel’s claim is that of ambivalence towards money’s role as an agent and fuel in this: On the one side, liberation from oppressive bondage of pre-modern societies. On the other hand, an interpretation of modern society, with its total immersion and focus on money, as being “inhuman”; people are “sensitive and nervous people”, alienated from others as they struggle for amassing more and more money – a struggle only a few succeed in and still fewer master fully.

Simmel’s explications are typical of a sociological discourse culture which is generally critical of numerous aspects of modern society which emerged when he lived, however, he is also critical to those who share his concerns, such as socialists and communists, accusing them of being flawed and simplistic in their analyzes and for promoting wrongful political solutions. However, what makes Simmel unique is his total focus on money, not technology, as the dynamic catalyst in social development, and the impact this has on how we feel, live and act, because modern money provide its owners an “..inner independence, the feeling of individual self-sufficiency” (Simmel 2001, p. 300). In this reasoning, Simmel claims a parallel between the development of money, which is becoming more and more generalized and abstract, and the development of social relations – and a fusion of the two factors: Money becomes “abstract group forces”, and for this reason “..the relationship of individual persons to others simply duplicates the relationship that they have to objects as a result of money” (Simmel 2001, p.301).

It is difficult to access the exact impact of Simmel’s thinking on social theory. Economists ignore him, in fact few economists are aware of his existence and his work. His reflections and explanations on the role of economy probably fall outside what is considered mainstream economic scholarship and research on money – Simmel would probably agree to this, as he himself indicated early in his book (p.54). However, among sociologists he is considered as one of the classical scholars, on par with Max Weber and Emil Durkheim, even if he is not so well known. According to one analyst, Simmel has gained increased recognition

during the 1990s because his interpretations of modern society – in spite of being almost 100 years old – in many ways anticipated and articulated the mentality of the post-modernist turn in social science, its general critique of modernity and reorientation towards subjectivity in explaining social development. What they identify as important is the question of trust, which also has a central role in Simmel's explanations, as this is essential for the status of money. As Arve Hjelseth (Hjelseth 2001, p. 59) has pointed out in his interpretation of Simmel, one may reasonably believe that trust is embedded in social relationships of the pre-industrial era, in closely knit, small scale and kinship organized peasant societies. As money economy develops and social relationships are transformed into money related economic relationships, people still need to trust one another, this is a matter of expediency at least. Simmel himself points to the crucial role of trust involved in extending credits – and, as an extension, the issuing and acceptance of cheques. As Simmel expounds this, he admits that trust is important, but explains this by drawing on an analogy to religion, i.e. as a matter of belief between two poles which cannot really see one another (Simmel 2001, p.460). Further, perhaps in order to reinforce this explanatory strategy of modern trust as a quasi-religious or metaphysical phenomenon, Simmel let his reasoning drift into an analysis of technology. Expressing himself basically in skeptically in terms of technology, he claims that “Just as, on the one hand, we have become slaves of the production process, we have become slaves of the products./.../Man has thereby become estranged from himself; an insuperable barrier of media, technical inventions, abilities and enjoyments has been erected between him and his most distinctive and essential being” (Simmel 2001, p. 483-484). However one may interpret this, Simmel seems unable to offer a satisfactory explanation of why trust still retains an important role in modern, money-based economy (which he admits), when the logic of money should dictate a “liberation” from the social bondage in which trust is inherent. Thus, the factor of religious belief is mobilized as an explanation – this also explaining why Simmel portrays man's relationship to technology as a type of religious bondage to technology, that which is a barrier between “him and his most distinctive and essential being”. Still, Simmel was one of the first social theoreticians who attempted a comprehensive treatment of money. Thus, one hundred years afterwards, with the almost total migration of money into electronic media – and with prospects for a further electronification of this with the smart card technology – how does Simmel's analysis stand?

Discussion: Money and smart cards

The uniqueness of Simmel is his focus on money as the medium and engine of social development, i.e. that the role of money, more so than technology or ideology, is the “engine” of development and primary cause of social change. The way money has become pervasive in society, in all types of social relationships, its “liberating” impact in terms of traditional social structures and dynamics, explains social development more adequately than other factors, according to Simmel. However, in expounding this, his analysis becomes pessimistic and critical as to the quality and desirability of what modern society has evolved into. Obviously, although his explanatory strategy is seductive, it seems farfetched to claim the existence of a

“distinctive and essential being” in mankind, a kind of *Urmensch* who becomes extinct by modernity. Although consumerism is a phenomenon of modernity, at times a type of compulsive behavior related to obtaining and possessing produced objects, which qualify as a religious credo or contemporary ideology – it is difficult to equate this with slavery, even if some elements of addiction may be observed, according to some analysts, among a few members of modern society, i.e. a minority. More fundamental, one may question the empirical foundation for his criticism of modern society: How could he possibly, without any empirical evidence apart from his own impressions, make his grandiose claims about modern people being “nervous” and acting “inhumane”? Furthermore, the implied contempt for the “liberation” that evolved following the dissolution of feudalism, this may well reflect his own, privileged position⁷⁶, which perhaps made the question of independence seem trivial for him. Still, if these interpretations and explanations are ignored as perhaps being misguided, reflecting more a general pessimism typical in some academic communities, his views on money are profoundly original. Using his explanatory strategy, it is logical to focus on trust and the point that value, even if social, has to be embodied in “something” substantial. The latter may be an institutional arrangement or some physical representation of this. If this is missing, the social legitimacy of money vanishes – this is an obvious prediction one may make by following Simmel’s logic.

The fiasco of anonymous electronic cash, as presented in the introduction of this chapter, i.e. the failure of DigiCash and others, and the difficulties other types of smart card based payment types have encountered is not so mysterious in view of Simmel’s reasoning: People – no matter how secretive they are - will distrust anonymous electronic cash precisely because it is anonymous. The ideas and concepts of DigiCash and others are logically flawed, in spite of the ingenuity of the cryptographically based software that David Chaum and others have developed: Their simplistic idea is based on the notion that banknotes and coins are “anonymous” because these leave no traces, i.e. they do not “smell”, thus they avoid the prying eyes of “Big Brother” and provide a type of privacy which most cherish. For this reason, champions of anonymous electronic cash claim their ingenious, cryptographically based cash will eliminate all traces. However, “anonymous” physical cash is really not anonymous – banknotes and coins have an identity and representation that is easy to recognize by those who use these, usually, as being bona fide and real. Electronic, anonymous cash, in contrast, is so anonymous that all these aspects are absent. In addition, the fear of counterfeits in an electronic world is perhaps one of the most sensible fears. Thus, in absence of an institutional guarantee, which also implies a type of bondage to someone or something, between a token that is presented as representing a certain value and someone else, then this token is worthless precisely because it is completely anonymous. Whereas this may plausibly explain why various schemes of “anonymous” electronic cash have failed (even as payment in the illegal economy), this may simultaneously explain why other types of electronic payment have had success. In these, there is an institutional backing; the electronic message that

⁷⁶ Simmel was rich, having inherited a considerable fortune, however, being Jewish, he was never fully accepted in the German academic community when he lived.

transfer money are trusted precisely because they have an identity and are traceable, i.e. they make visible the link that guarantees the authenticity of the information provided, in effect, this information is bona fide value transfer, just as genuine as handing over a real banknote. This may explain the general popularity and diffusion of electronic payment in the shape of debit and credit cards that transfer funds within and between financial institutions and act as intermediaries between people who transact. The success of various electronic payment services such as PayPal, eWire, etc. are due to the fact that their business models are based on providing similar services much faster than the traditional financial institutions are capable of, however, these depend on the latter – and they do not transfer "anonymous" electronic cash.

Extending this even further, one may claim that the petty cash function which are provided in some smart cards owe their existence to the fact that these are not anonymous; these means of payment communicate clearly what and whom they represent, as evident in the concept of mobile commerce (m-commerce), which uses the mobile telephone handset as a "purse". For the same reason, various schemes based on the idea of community currency⁷⁷, which adherents claim are viable, are strongly based on the trust factor, i.e. a clear identity and institutional foundation associated with this. These types of money, which are aligned with communitarian ideals and activism, however, contradict some of the assumptions that Simmel based his analysis of modern society, such as the general dissolution of social bonds and solidarity. Still, the factors of trust, as expressed in the networks of reciprocities, are basic in these. Various known as community currency or local currency, according to adherents, these types of money have had success in places that lack official money, due to poverty and unemployment, such as the Local Exchange Trading Scheme in the UK⁷⁸.

In spite of this, one may envisage that there may be a need for the type of anonymity that banknotes and coins provide, however, in an electronic medium. In a way, this exists in the prepaid memory cards that use some elements of smart card technology: It is impossible to trace the identity of a person who uses these cards in public payphones from data on the card. According to an article in the journal *Card World Independent*⁷⁹, there has been a rapid growth in the demand for "gift cards", i.e. prepaid Internet access cards, using technology identical to prepaid payphone memory cards. As with ordinary gift cards, these may also be used in stores and hotels for payment, however, according to the article, these cards have become popular for payment of access to pornographic sites on the Internet. By using these instead of credit cards, the telltale and embarrassing evidence on credit card invoices are hidden, i.e. by-passed. According to the article, two to three million cards of this type are in circulation in the USA (in 2001). These cards are embossed and printed with logos and other signs that make their identity plain, thus they are not anonymous, however, their use do not "compromise" the identity of the person who uses them.

⁷⁷ Cf. Bernard Lietaer, "The future of money: Creating new wealth, work and a wiser world", in www.transaction.net/money/book/

⁷⁸ Cf. Gill Seyfang, "The Euro, the pound, and the shell in our pockets – Rationales for complementary currencies in a global economy", in <http://website.lineone.net/~gillseyfang/cerise/ccnpe.htm>

⁷⁹ "Need for anonymity leads to establishment of a significant niche business card", in February 2001, p. 6.

In terms of technological diffusion, what is remarkable is the temporal aspect, the slowness by which applications like these are developed. Furthermore, what is remarkable is that these are used without any type of virtual key for the access these provide. Even if these types of money have a clear identity, which make them bona fide as payment, they still provide its users with anonymity and liberty. In terms of monetary categories, these may be classified as "special-purpose money", because their liquidity is restricted, in contrast to generalized money, which in theory, may be used for all types of payment. Contrary to what one may think, there has been a growth of special-purpose money in recent years, under the concept of "loyalty"-programs. Thus, most airlines have frequent fliers bonus systems, which may be used for flying even more by those who are entitled, i.e. their convertibility is restricted. Some claim that this is an ingeniously smart way for the airlines to bribe its customers. Keeping track of the credits that people accumulate in these programs has become an important area for the focus of the smart card industry; they are trying to convince loyalty program operators that smart card technology – instead of magnetic stripe cards that are most common now – will give them numerous advantages, both in strategic and economic terms. So far they have had little success with this, however, they claim that by using a smart card technology, the concept of "value network" and its associated "club"-concept becomes more feasible because of multi-application cards. This idea, as evident in the views of the informants of the telecom service cluster presented in the last chapter, is apparently a concept that is still in its infancy. However, in concepts like these, the anonymity of the prepaid cards is absent. On the contrary, one may claim that a loyalty program that records all transactions made by a person in order to allocate rewards, reintroduces a type of bondage that is very compelling. Thus, turning to the concept of virtual keys and locks, one may wonder who is keeping whom under lock, and who really is in the possession of the key.

7 Conclusion: Explaining virtual keys

The shift in focus and increased complexity

As explained in the introduction of this report, the choice of virtual keys was made because this was believed to be *strategic*, i.e. it would allow a delimitation of the study while simultaneously allowing an analysis of a number of dimensions involved in the development and diffusion of ICT. However, as the inquiry evolved, the focus of the study gradually shifted away from laboratories that develop virtual keys – towards the industry as a whole, i.e. the "external design parameters" ruling the design, construction and diffusion of virtual keys, in particular as these are embodied in smart card technology. Thus, the inquiry gradually shifted its focus to smart card technology and the industry, markets and social systems associated with these. One reason for this was the phenomenon of "dominant design", which at present has stabilized numerous technological aspects related to virtual keys. Another reason for this shift relates to the strong alignment of virtual keys to ICT *systems*, with variable degrees of complementarity and interdependence.

In spite of this shift in the focus of analysis as the inquiry progressed, it maintained its initial goal of comparing virtual keys with pre-ICT equivalents such as mechanical and information based keys and locks. The idea of this was to analyze virtual keys within the dichotomy of continuity and discontinuity in technological development. Because locks and keys, as regulation technologies, have existed for thousand of years, a comparison of these with the ICT-based virtual keys would show to what extent the latter are novel, i.e. may possibly represent technological discontinuity or a radical innovation. Furthermore, the relationship between smart card technology and its functions as an instrument of payment (money) gradually emerged as significant. Thus, an inquiry that began with a primary focus on design in the laboratory evolved and finally ended up with an analysis of money and its role in society. In the course of this, in spite of the delimitations initially set on the topic of inquiry, the large volume of empirical evidence (the avalanche of facts) caused an exponential increase in the complexity of the analysis.

In concluding this inquiry, an attempt will be made to confront the findings presented in the previous chapters, with the starting point, the initial claim that although contemporary theories provide interesting and illuminating explanations of some aspects related to how ICT is created and developed, in terms of explaining salient characteristics of ICT, these are only partly successful. The inquiry of the virtual keys was motivated by a quest for exploring new ways of explaining how technology, in particular ICT, is developed, mainly because current theories do not adequately explain the development and diffusion of ICT. One reason for this may be that these theories were developed in a pre-ICT era. Now the question to pose is: Does the study presented in this report of virtual keys really contribute to a new understanding of how ICT-technology is developed and diffused? Or, does it only beg for more answers? In the following sections, an attempt to answer these questions will be made, first by making a general summary of the empirical results, then by discussing these in a theoretical perspective.

SIM-cards and other smart cards

Providing an overview implies simplifying, i.e. cutting away details, exceptions and rich nuances, in effect brutally stripping off much material in order to make apparent a few salient and essential features. One of these may be the fact that smart cards technology has been most successful as SIM-card in the mobile handset of GSM mobile communication system. As pointed out in chapter 5, 65% of the 2001 shipment of smart cards from the industry was destined to the telecommunication sector, i.e. to the GSM-system. In the world, as the GSM-system has a total dominance in Europe and has increasingly been adopted outside Europe, in particular in Asia, the diffusion of smart cards qua SIM-cards have piggy-backed on this, so that the dominant use of smart card technology is in mobile communications. According to one reliable source⁸⁰, at the end of June 2002, there were 721 million GSM customers in the world, serviced by 438 mobile communication operator-licensees in 157 countries. By incorporating the smart card in the design of the GSM-system in the early 1980s⁸¹, the designers in fact introduced “intelligence”, or more accurately, independent processing capability and memory in the mobile handset, for a number of reasons. One reason is implied by the meaning of the acronym SIM, i.e. this meaning “Subscriber Identity Module” – that this would serve as a key to the mobile communication system, it would authorize the user and give him or her access to the system. It was also designed to generate the cryptography, i.e. the “private” encrypting of encrypted digital signals that makes it almost impossible to decipher the contents of a message by intercepting radio signal in the air. In addition, in the SIM-card’s memory, it is possible to store information, such as phonebooks and software. Apart from the fact that this represents a technological discontinuity in the development of key technology, thus being an important attribute in classifying GSM as a radical innovation, this is truly a virtual key. In fact, trying to interpret the SIM-card as based on antecedents and predecessors among mechanical locks and keys only distorts the novelty of this innovation. In terms of design, the SIM-card has become standardized and “frozen” in the GSM 11.11 standard, which is very similar to the ISO 7816 standard for smart cards. The reason for this kinship (or technological sisterhood) is that the idea of creating the SIM-card was strongly influenced by the smart card; in the early 1980s in the ICT community there was much attention and enthusiasm as to the potential application of the emerging smart cards.

⁸⁰ The *GSM Association*, cf. their Web-site: <http://www.gsmworld.com>

⁸¹ At that time, the work undertaken to design what is now known as GSM was undertaken in a technical committee of the European standardization organization CEPT, predecessor of ETSI (European Telecommunications Standardization Institute). In the CEPT-system, the official name of this committee was “Groupe special de mobilité” in French – hence the abbreviation GSM – which has now been renamed as representing “Global System of Mobilecommunications”.

A complementary, if not officially admitted reason for adopting the smart card in the design of GSM was the idea of “plastic roaming”⁸². In this, the subscription to the GSM and payment for its use was embodied in the SIM-card, this tiny piece of plastic, not in the handset. The idea of this was to separate subscription as a customer relationship (in effect, a social relationship) from the hardware implementation, because the designers of GSM were apprehensive as to how much the handset would cost. At that time, the GSM mobile handsets were non-existent, they were just an idea in the minds of these engineers, however, the first generation handsets, such as those used in the NMT (Nordic Mobile Telephone), cost approximately ten times more than today (twenty years afterwards – adjusted for inflation). In addition, these were still very heavy and voluminous, in comparison with handsets of today. The designers feared that the future GSM handset could be even more expensive because of uncertainties as to the cost of GSM’s technology. In this, the designers thought that making a split enabled by introducing the SIM-card would make GSM more attractive, because then users could share a mobile handset and still maintain separate user identities in the system, this being done simply by inserting the SIM-card into the handset. This concept may have been inspired by the sharing of hardware as evident in public payphones and ATM-terminals, to be used when needed.

Just how much the SIM-card has contributed to the success of the GSM is perhaps impossible to estimate, however, at the time of its design, it provided the handset with computational capabilities, i.e. made the handset “intelligent”, with the type of development potential that now give the mobile communication operators the opportunity to become players in the emerging m-commerce arena. Thus, controlling the SIM-card also give mobile operators a strategic advantage which they are now trying to develop. In contrast, as pointed out in chapter 5, equipment manufacturers claim that the SIM-card is really superfluous; in most handsets these are fixed, or “glued” and never removed – the functions provided by the SIM-card could just as well be integrated with the hardware of the handset, not as a separate entity.

In contrast, in the financial sector, institutions such as banks and credit card companies have slowly and reluctantly evolved towards adopting smart card technology; their official policy is a total migration in 2005-2008. The main reason for this is that the keys used at present, which are predominantly magnetic stripe cards combined with PIN-codes, are technologically “dumb” in comparison with smart card technology. Thus, magnetic stripe card users have increasingly become victims of various fraud schemes. Even if this, the

⁸² The term “roaming” in mobile communications refers to the process by which the mobile communication system undertakes a search in order to locate the position of a mobile handset in the topography, to find out which radio cell this is currently covered by, in order to allocate a channel (radio frequency) for the communication process. The roaming process is essential because this gives the system precise information as to the location of the mobile handsets, or mobile stations, as the engineers prefer to call these. The term “plastic roaming” was a colloquial, somewhat ironic and unofficial term used by mobile communication engineers in the discussions that decided to incorporate the smart card in the design of the mobile system.

money lost to fraud, still may not amount to much⁸³, the institutions fear that the image of security, which is essential for the trust factor, may become tarnished and compromised by the increasing number of fraud cases. Often cases like these, as reported in the media, are amplified by customers who claim that the institutions attempt to deny their liability and responsibility; being a victim of fraud is exacerbated by the bank or the credit card company that either tries to evade their responsibility or blame customers for being irresponsible, in fact, indirectly contributing to the success of the fraud. Still, making copies of genuine magnetic stripe cards is relatively simple and has become the source of a criminal growth industry in many countries, for which reason there is a concern, “something must be done”. However, the attitude is not enthusiastic towards smart cards as an alternative, mainly because these will incur heavy investments, according to their estimates.

As evident in chapter 5, the reason for their attitude may also be due to their basic perceptions of ICT as a system for financial services. Being strong adherents of centralized systems enabling the grand ledger, most of these trace their ancestry back to IBM’s golden age of gigantic corporate computing centers. This may explain their inclination, which they convincingly justify, to the advantages of serving their customers from their computing fortresses. In their mind, the challenge is to provide absolute secure access to their systems, in which the question of virtual keys is mainly considered as ensuring the authenticity of the users and their authorization of transactions. All the other potentials of smart card technology they think may be more efficiently and flexibly served by means of their system – the economy of scale made possible in these are of a different order than those envisaged by various applications residing in smart cards. Needless to say, this attitude is in harmony with their basic interest; having control of the flow of money within their systems and spheres of influence is vital for their business. Thus, whereas the mobile communication industry adopted the smart card in its technological infancy in the early 1980s, the financial service sector is slowly adopting this, as a “mature” technology more than twenty years later.

According to the shipment figures of smart cards from the smart card manufacturing industry, two sectors, telecommunications and finance, in 2000 accounted for 92% of the 600 million smart cards sold this year. Of this, nearly three quarters went to the telecommunications sector. Until recently, a substantial part of the financial sector’s use of smart cards has been in France, a fact that reflects a national idiosyncrasy, i.e. the generally strong position of smart cards in France. Whereas the development dynamic of the mobile communication sector and its early adoption of smart cards may be adequately explained in terms of this sector’s *innovation regime* (Godoe 2000) capable of creating radical innovations, the financial sector’s gradual, almost feet-dragging drift towards adopting smart cards may be characterized as incrementalism, reflecting a number of factors, of which a generally

⁸³ Cf. *Card World Independent*, February 2001, p.1, article “Online plastic card fraud “less than expected””. The article claims that card fraud losses incurred in the UK in 2000 by banks and financial institutions were approximately UK£ 300 million, or 0,145% of their turnover. Considered as an operational cost, this is negligible, and compared with the costs of investing in “more secure” technology and infrastructure, this is still inexpensive.

conservative culture seems prominent. However, an important reason for this sector's decision to migrate to smart card technology is that a few dominant actors – MasterCard, Europay and VISA, who also are most exposed to the increase of magnetic stripe cards frauds – made a policy decision on this, in 1998. Being powerful, they provided a technological leadership and authority (Chesbrough and Teece 1996), which the sector, because of its structure and culture, was incapable (in effect, not interested because they were comfortable with the magnetic stripe card solution) of organizing by them. In a perspective of innovation regimes, in contrast to the telecommunication sector of the 1980s, the financial sector's innovation regime is weak, almost absent, as evident in the anachronisms one may observe in the large banking sector in the USA. In effect, a similar situation is evident in EU's eEurope initiative of promoting the diffusion of smart card technology by employing a rhetoric praising the virtue of a market driven dynamic. In fairness, the EU should be given the benefit of doubt as to the likelihood of this policy having success, however, judging from the progress of this initiative, even coming close to the targets set for 2003 may require multiple miracles. In a perspective of innovation regime, the leadership and organizational capability provided by the EU is even weaker than the financial sector's.

Now, using the strongly simplified account presented above of how virtual keys in smart cards technology has been developed and diffused in two important sectors, the mobile communication sector and the financial service sector, how may this be explained by current theories that approach design, construction and diffusion of new technology? An analysis and discussion of this will be attempted in the next section.

Virtual keys and current theories explaining technology

In chapter 2, a review was presented of various theoretical approaches that attempt to explain the design, construction and diffusion of new technology. Among the approaches reviewed, two were identified as being important because of their dominant position as explanatory strategies: The social constructionist theories and optimization theories. It was claimed, and by this predicted, that neither of these would provide satisfactory explanations of why and how virtual keys are developed and diffused. However, the approach that perhaps most successfully could explain this is the one advocated by Bruno Latour, in his actor-network theory (ANT), specifically his ideas of analyzing the development and diffusion process as a series of translations processes (Latour 1987), which is much more interesting than his strange experiment in adopting methods from linguistics for this purpose. In his theory of translation processes, for achieving success, the technology has to become indispensable to society, which is the ultimate goal. In the discussion in chapter 5 of Latour's theory, it was claimed, as earlier, that replicating Latour's approach, even if appealing, may be difficult, and that the classic explanation of diffusion provided by Everett Rogers (Rogers 1995), even if criticized by Latour, is more flexible and manageable. Furthermore, it was claimed that Rogers' explanations are in fact not very different from Latour's – one may even suspect that Latour has been much more influenced by this than he admits. For this reason, Rogers' concept of

contingent innovation-decision is interesting, even more so if this is qualified by introducing the system aspect in the analysis: Making decisions on a system level, the growth of smart card technology is based on *market-oriented* authority innovation-decisions, which is complementary to, and interacts with, *system-dependent* contingent innovation-decisions, often in conjunction with other types of innovation-decisions.

Thus, what is difficult in both Rogers' and Latour's approaches are an adequate understanding and explanation of how different systems function in terms of emerging new technologies. This is accentuated by the fact that in terms of virtual keys, smart card technology is identical in both systems discussed above, i.e. the financial sector and the mobile communication sector. By introducing the conceptual framework of *innovation regimes* (Godoe 2000), i.e. that different sectors and industries have different innovation regimes: Some innovation regimes are strong, technologically radical and politically influential, as in the telecommunication sector in the 1980s, prior to the onset of deregulation of this industry. Others are weak, feeble or conservative, as evident in the financial sector and a number of other industries, e.g. the automobile manufacturing industry. The reasons for this are complex, however, fiercely competitive markets may, contrary to what many libertarians think, contribute to the dilution or weakness of an innovation regime. In the previous section, comparing the evolution of smart card technology based virtual keys in the telecommunications sector and the financial service sector, it was claimed that the early adoption of smart card technology could be explained by the telecom sector's innovation regime in the early 1980s.

In the landscape of theories that attempt explaining the emergence, development and diffusion of new technology, in particular in the social constructionist community, Latour is unique and original. However, he competes with numerous others in providing explanation – the social constructionist community is theoretically highly heterogeneous in terms of a variety of approaches and methodologies, even if they loosely share a common, basic assumption as to the primordial status of social and cultural factors in explanations. Thus, some of these approaches, such as the idea of analyzing technology “as text”, or as metaphors and narratives, may provide some insight, specifically in terms of how people perceive a new technology – and why they adopt, reject or modify this, i.e. how new technology is used or “domesticated”. In the case of virtual keys and smart cards, as evident in the interviews of the project leaders of large smart card projects in Norway, a number of different perceptions exist, i.e. this complies with what social constructionists claim as technology having interpretive flexibility – or, to put this in plain language, technology means different things to different people, depending on their location in time and space and who they are. These approaches may have an interesting potential in penetrating into the structure and system of belief that cloud various optimization theories used by players in the virtual key and smart card industry. An interesting case would be to analyze the ideas that constitute the notion of a “business case”: Why do some claim that there is “no obvious business case for smart card technology”, whereas others claim the opposite, however, both mobilizing an almost identical rhetoric of rationalism and utility function maximizing, i.e. the core of optimization theory. Interesting as the results of these types of inquiries may be, they would nevertheless fail to

adequately explain the emergence and diffusion of new technology, in this case, the development and diffusion of virtual keys and smart card technology.

Thus, in turning our heads in order to look towards the community of optimization theory, the strength of these is not trying to explain why a new technology emerges or diffuses, even if understanding this should be basic for the prescriptions they advocate, i.e. recommending methods and approaches for how to create new technology. In spite of this, some of the basic tenets of this approach, as articulated by Herbert Simon in his *sciences of the artificial* (Simon 1969), bear resemblance to many of the positions advocated by the social constructionists, as pointed out in chapter 2. Furthermore, some of the prescriptions that Herbert Simon made in terms of methods, i.e. how to find the best utility function of a design, have become economically and technically feasible by means of advanced ICT, such as rapid prototyping machines, CAD, visualization “tools”, simulation software, etc. The impact of these, combined with increased standardization of technological components and technology “platforms”, explains why the nature of modern design, product development and related R&D has changed during the 1990s, even in the field of designing virtual keys, as explained in the first chapter of this report. Thus, as various “dominant designs” become hegemonic in product development and technology design, the diffuse notions of “external design parameters” become increasingly important. These factors are elusive and capricious; they are generated by the environment of the firm and the technology, by society and culture – mediated by inarticulate market signals. For this reason, one may predict, as evident in many R&D organizations in the ICT industry, that these will invest more in activities that attempt to interpret and translate these external factors into tangible design parameters. Soon they may discover the utility function of social constructionist approaches to technology.

The impact of virtual keys

For most people, the virtual keys and the technology in which these are embedded, are “black boxes”; one may even term these as “invisible boxes”, because people are usually totally unaware of, or disinterested in, their existence. Their interface with systems that use these are usually through PIN-codes and passwords; these are mushrooming, just like more and longer telephone numbers, passwords that require periodic change, email-addresses, URLs, etc. Not only are they a nuisance – for many they may create serious problems, as evident in shops where elderly momentarily “black-out”, as they are straining and often fail to remember the PIN-code of their credit card. (This too often happens with young people.) If the bank suspects that a person has had a slip of paper with the PIN-code written on this, in a stolen wallet containing the credit card, then they will claim negligence on part of the customer and refuse to compensate the illicit use of the card. For many, losing a mobile phone is serious mostly because of the information stored in the SIM-card; in contrast, the handset of the mobile phones are dispensable because they are relatively inexpensive and may be ditched when the battery is worn out. Thus, in modern society, the virtual keys are becoming just as indispensable as mechanical keys; one may even envisage that in the future, the latter will

disappear or have a diminishing importance as private homes, filing cabinets and cars are equipped with locks using virtual keys.

On a general level, virtual keys constitute a *regulation technology* because these are designed in order to discriminate or differentiate people and their actions; the possession of a key is an authorization as to what that person is at liberty to do or access. Viewed in an evolutionary perspective, most societies have designed and implemented various regulation technologies for thousands of years, as evident in the archaeological remains from Egypt and Mesopotamia. In spite of these predecessors and antecedents, the new virtual keys and the technologies they are embodied in, represent radical innovations – they represent technological solutions that were not possible prior the emergence of ICT. Because regulation technologies are products of engineering design, they may also be *deregulated*, as evident in the technically skillful actions of hackers (Godø 2002). Essentially, virtual keys are closely related to the proprietarization of the virtual world, what Bruce Sterling (Sterling 1992) calls the ownership of the unreal real estate of cyberspace. As our lives increasingly migrate into cyberspace and territories within these that control our lives on the outside, in real space, the virtual keys and their regulation technologies become increasingly more important as social and political issues. Possibly, the concerns that many have about a “digital divide” that will differentiate people in society will increasingly become a question of how the various virtual keys are designed – who and what these discriminate, differentiate, or control – and who masters these. One may envisage that numerous questions that will emerge: What is “property” in cyberspace? Who owns this or is allowed to control this? What is freedom? In the conversion of regulation technologies into a virtual world, many of our ideas of value may require rethinking and redefinition, thus we need to develop a new understanding of what needs to be regulated and why – and by whom.

Literature

- Abernathy, W. J. and K. B. Clark (1985). "Innovation: Mapping the winds of creative destruction." Research Policy **14**: 3-22.
- Akrich, M. and B. Latour (1992). A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. Shaping technology/Building society - Studies in sociotechnical change. W. Bijker and J. Law. Cambridge, Massachusetts, The MIT Press: 259-264.
- Andreasen, M. M. and L. Hein (1986). Integrert produktutvikling. Oslo, Universitetsforlaget.
- Basalla, G. (1988). The evolution of technology. Cambridge, Cambridge University Press.
- Bijker, W. E., T. P. Hughes, et al., Eds. (1987). The social construction of technological systems: New directions in the sociology and history of technology. Cambridge, Mass., MIT Press.
- Bucciarelli, L. L. (1988). "An ethnographic perspective on engineering design." Design studies **9**(3): 159-168.
- Chesbrough, H. W. and D. J. Teece (1996). "When is virtual virtuous? - Organizing for innovations." Harvard Business Review(January-February): 65-73.
- Cooper, R. G. (1996). New Products: What Separates the Winners from the Losers. The PDMA Handbook of New Product Development. R. e. al. New York, John Wiley & Son: 3-18.
- Cooper, R. G., Scott J. Edgett, et al. (2000). "New Problems, New Solutions: Making Portfolio Management More Effective." Research Technology Management **43**(2): 18-33.
- Dosi, G. (1988). "Sources, procedures and microeconomic effects of innovation." Journal of economic literature **xxvi**: 1120-1171.
- Dubinskas, F. A. (1988). Making time - Ethnographies of high-technology organizations. Philadelphia, Temple University Press.
- Feldman, M. S. and J. G. March (1981). "Information in Organizations as Signal and Symbol." Administrative Science Quarterly **26**: 171-186.

- Ferguson, E. S. (1993). Engineering and the mind's eye. Cambridge, The MIT Press.
- Freeman, C. and C. Perez (1988). Structural crisis of adjustment, business cycles and investment behavior. Technical change and economic theory. G. D. e. al. London, Pinter Press: 38-66.
- Gibbons, M. (1994). "Transfer sciences: Management of distributed knowledge production." Empirica **21**: 259-270.
- Gibbons, M., C. Limoges, et al. (1994). The New Production of Knowledge: The dynamics of science and research in contemporary societies. London, Sage.
- Godøe, H. (2000). "Innovation regimes, R&D and radical innovations in telecommunications." Research Policy **29**: 1003-1046.
- Godø, H. (1993). Telenasjonen Norge i 2003. IT neste TI - Informasjonsteknologi de neste ti år. P. Gottschalk. Oslo, Ad Notam Gyldendal: 223-230.
- Godø, H. (1999). Hacking som fenomen. Oslo, Norsk institutt for studier av forskning og utdanning: 41.
- Godø, H. (2001). Mobilkommunikasjon, smalbåndsrevolusjonen og telegrafiens renessanse - Fremveksten av en ny type sivilt samfunn? Oslo, NIFU - Norsk institutt for studier av forskning og utdanning: 14.
- Godø, H. (2002). "Rethinking Computer Hacking." (forthcoming) VEST - Journal for Science and Technology Studies.
- Goody, J. (1977). The domestication of the savage mind. Cambridge, Cambridge University Press.
- Grint, K. and S. Woolgar (1997). The machine at work. Cambridge, Polity press.
- Henderson, K. (1991). "Introduction: Social studies of technological work at the crossroad." Science, Technology and Human Values **16**(2): 131-139.
- Hjelseth, A. (2001). "Pengenes forutsetninger og konsekvenser - Simmel som økonomisk sosiolog." Sosiologi i dag **31**(3): 45-68.
- Kahn, D. (1996). The Codebreakers - The story of secret writing. New York, Scribner.

Knorr-Cetina, K. D. (1981). The Manufacture of Knowledge - An Essay on the constructivist and contextual nature of science. Oxford, Pergamon Press.

Latour, B. (1987). Science in action - How to follow scientists and engineers through society. Boston, Harvard University Press.

Latour, B. (1992). Where are the missing masses: The sociology of a few mundane artifacts. Shaping technology/Building society - Studies in sociotechnical change. W. Bijker and J. Law. Cambridge, Massachusetts, The MIT Press: 225-258.

Latour, B. and S. Woolgar (1979). Laboratory life - The social construction of scientific facts. London, Sage Publications.

Law, J. and W. E. Bijker (1992). Postscript: Technology, stability and social theory. Shaping technology/Building society. W. E. B. a. J. Law. Cambridge, Massachusetts, The MIT Press: 290-306.

Lee, J.-R., D. E. O'Neal, et al. (1995). "Planning for dominance: a strategic perspective on the emergence of a dominant design." R&D Management 25(1): 3-15.

Levy, S. (2001). Crypto. London, Penguin Books.

Lie, M. and K. H. Sørensen, Eds. (1996). Making technology our own? - Domesticating technology into everyday life. Oslo, Scandinavian University Press.

Malmanger, M. (2000). Kunsten og det skjønne - Vesterlandsk estetikk og kunstteori fra Homer til Hegel. Oslo, Aschehoug.

McAloon, T. C. and A. J. Robotham (1999). A framework for product development. Critical Enthusiasm - Contributions to design science. N. H. Mortensen and J. Sigurjonsson. Trondheim, P2005 - Norwegian Research Council: 83-98.

Mokyr, J. (1990). The lever of riches - Technological creativity and economic progress. Oxford, Oxford University Press.

Nowotny, H., P. Scott, et al. (2001). Rethinking Science: Knowledge and the public in an age of uncertainty. Cambridge, Polity Press.

- Pool, I. d. S. (1983). Forecasting the telephone: A retrospective technology assessment. Norwood, Ablex.
- Rogers, E. M. (1995). Diffusion of innovations. New York, Free Press.
- Rosenberg, N. (1994). Exploring the black box. Cambridge, Cambridge University Press.
- Sahal, D. (1985). "Technological guideposts and innovation avenues." Research Policy **14**: 61-82.
- Seippel, Ø. (2001). "Natur, estetikk, politikk: Mellom sosiologisk postmodernisme og moderne naturestetikk." Sosiologisk tidsskrift **9**(3): 135-155.
- Simmel, G. (2001). The Philosophy of Money. New York, Routledge.
- Simon, H. (1969). The sciences of the artificial. Cambridge, Massachusetts, The MIT Press.
- Simon, H. A. (1992). The Science of Design: Creating the Artificial. The Immaterial Society - Design, Culture, and Technology in the Postmodern World. M. Diani. Englewood Cliffs, New Jersey, Prentice Hall: s 83-101.
- Sterling, B. (1992). The Hacker Crackdown. New York, Bantam Books.
http://www.eff.org/Publications/Bruce_Sterling/Hacker_Crackdown/
- Utterbach, J. M. and F. F. Suarez (1993). "Innovation, competition and industrial structure." Research Policy **22**: 1-21.
- Vincenti, W. G. (1995). "The technical shaping of technology: Real-world constraints and technical logic in Edison's lighting system." Social Studies of Science **25**: 553-74.
- Walsh, V. (1995). "The evaluation of design." International Journal of Technology Management **10**(4-6): 489-510.
- Winner, L. (1993). "Social constructivism: Opening the black box and finding it empty." Science as culture **3**(3): 427-452.
- Wynne, B. (1975). "The rhetoric of consensus politics: A critical review of technology assessment." Research Policy **4**: 108-158.
- Yin, R. K. (1989). Case study research - Design and methods. Newsbury Park, California, Sage Publications.